User Manual

YOYO**Router**
Mobile Travel Router EE1

Versatile multi-function router with Wi-Fi, Ethernet
and USB Modem support

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

V1.00

Table of contents

COPYRIGHT **1**

FCC INTERFERENCE STATEMENT **2**

CHAPTER 1 INTRODUCTION **5**

1.1. Package List 5
1.2. Hardware Overview 5
1.2.1. Front Panel 5
1.3. LED indicators 6

2. GETTING STARTED **7**

2.1. Operating Modes 7
2.2. Preparing YOYORouter EE1 8
2.3. Connecting to YOYORouter EE1 10
2.4. Accessing the status and configuration pages. 10
2.5. Setting up YOYORouter EE1 in Wireless WAN Mode 11
2.6. Setting up YOYORouter EE1 in Ethernet WAN Mode 13
2.7. Setting up YOYORouter EE1 in Ethernet WAN Mode with Failover 14
2.8. Setting up YOYORouter EE1 in Share Mode 16
2.9. Wi-Fi Configuration Tips 17
2.10. Connecting to the YOYORouter using WPS 17

3. CONFIGURATION REFERENCE GUIDE **18**

3.1. Using the Setup Wizard 18
3.1.1. Starting the Wizard 18
3.1.2. Configure Settings using the Wizard 19
3.2. Advanced Settings 22
3.2.1. Basic Setting Group 22
3.2.1.1. Network Setup 23
3.2.1.2. DHCP Server 37
3.2.1.3. Wireless Settings 39
3.2.1.4. Change Password 42
3.2.2. Forwarding Rules 43
3.2.2.1. Virtual Server 43
3.2.2.2. Special AP 44
3.2.2.3. Miscellaneous 45
3.2.3. Security Setting 46
3.2.3.1. Packet Filters 46
3.2.3.2. Domain Filters 48
3.2.3.3. URL Blocking 49
3.2.3.4. MAC Control 50
3.2.3.5. Miscellaneous 51
3.2.4. Advanced Setting 52
3.2.4.1. System Log 52
3.2.4.2. Dynamic DNS 53
3.2.4.3. QOS 54

3.2.4.4. SNMP 55
3.2.4.5. Routing 56
3.2.4.6. System Time 57
3.2.4.7. Scheduling 58
3.2.5. Tool Box 59
3.2.5.1. System Info 59
3.2.5.2. Firmware Upgrade 60
3.2.5.3. Backup Setting 60
3.2.5.4. Reset to Default 60
3.2.5.5. Reboot 61
3.2.5.6. Miscellaneous 61
4. TROUBLESHOOTING 62
4.1. Basic Problems 62
4.2. Wi-Fi Problems 62
4.3. Problems with the Mobile Broadband Connection 64
4.4. Other Problems 66
APPENDIX A LICENSING INFORMATION 67

Chapter 1 Introduction

Congratulations on your purchase of a YOYORouter EE1. This product is specifically designed for mobile user who needs to have the Internet access beyond his home and office

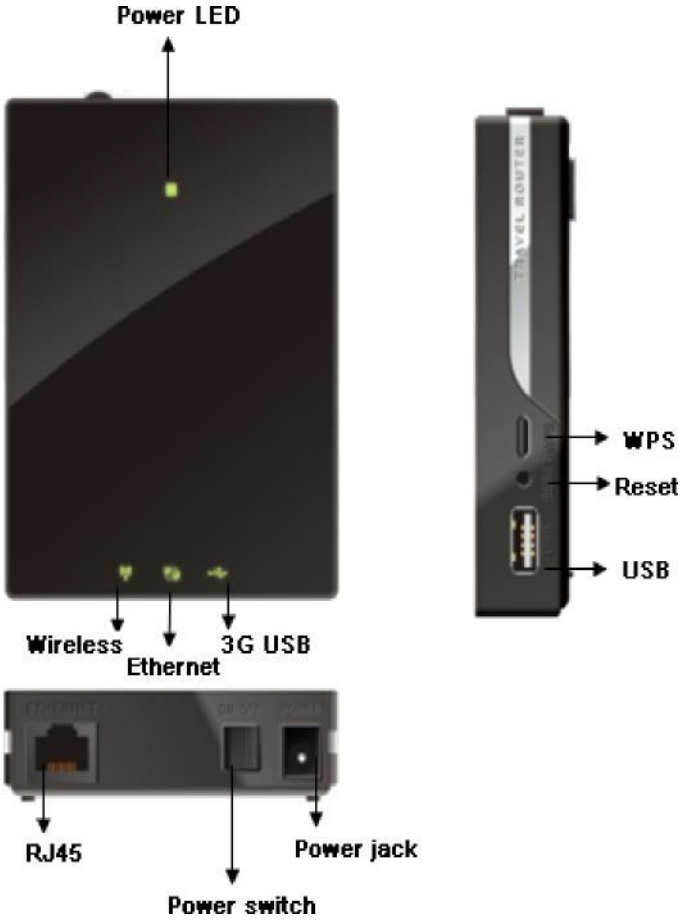
The Quick-Start Guide shows how to get up and running with the YOYORouter EE1. This User Guide provides in-depth instructions to use all of the features.

1.1. Package List

Items	Description
1	YOYORouter EE1
2	Power adapter 5V 2A
3	Lithium ion battery
4	CD-ROM
5	Quick-Start Guide

1.2. Hardware Overview

1.2.1. Front Panel



1.3. LED indicators

Battery and Power status	
	Battery is fully charged (power on)
	Battery is powering the router
	Battery is on charge or no battery is installed
	Battery low
Off	Battery is fully charged (charger connected and power switch off)

Wi-Fi Status	
	Wi-Fi (WLAN) is on
	Data transfer over Wi-Fi
	Fast flash denotes WPS mode

Ethernet (WAN or LAN connection)	
	Cable plugged in, connection established
	Data transfer over Ethernet

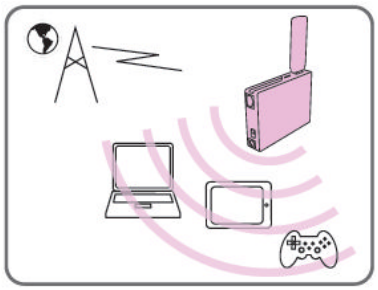
USB	
	USB Modem is on
	Data transfer over USB Modem

For any indicators on the USB Modem, please consult the documentation from the manufacturer.

2. Getting Started

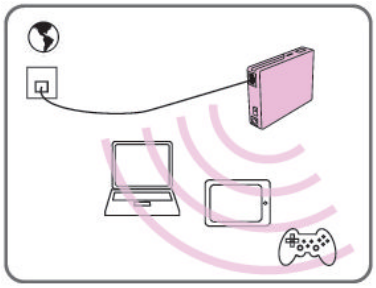
2.1. Operating Modes

YOYORouter EE1 has four operating modes to keep you connected via cabled Ethernet WAN (Wide Area Network), Wireless WAN (Mobile Broadband) or Wi-Fi hotspot sharing:



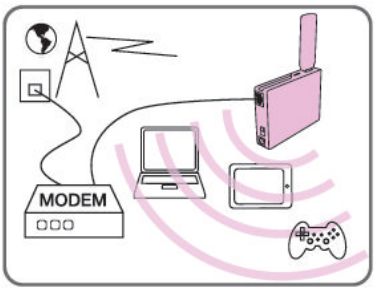
Wireless WAN (Mobile Broadband) Mode
Make a Mobile Broadband connection using LTE/HSPA/HSDPA/UMTS/EDGE/GPRS via a USB modem (USB dongle) plugged in to YOYORouter EE1. Share it via Wi-Fi and Ethernet.

YOYORouter EE1 is compatible with a wide range of popular USB modems including Huawei®, Novatel Wireless™, Option®, Sierra Wireless®, ZTE® and others.



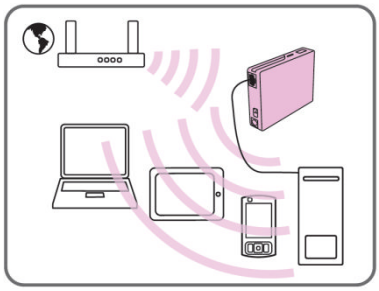
Ethernet WAN Mode
Connect to a cabled Ethernet WAN connection such as an ADSL or cable modem, hotel or office cable facility – share it with multiple Wi-Fi devices. Great for connecting portable devices that do not have an Ethernet port.

(Hotel/office cable connection illustrated)



Ethernet WAN Mode with Failover
Operate in Ethernet WAN Mode and automatically switch over to Wireless WAN Mode if the cabled WAN connection fails.

(ADSL/Cable modem WAN illustrated)



Share Mode
Connect to an existing Wi-Fi Network and share that connection with multiple users via Wi-Fi and Ethernet. YOYORouter EE1 can be used to connect a device that only has an Ethernet port to a Wi-Fi network.

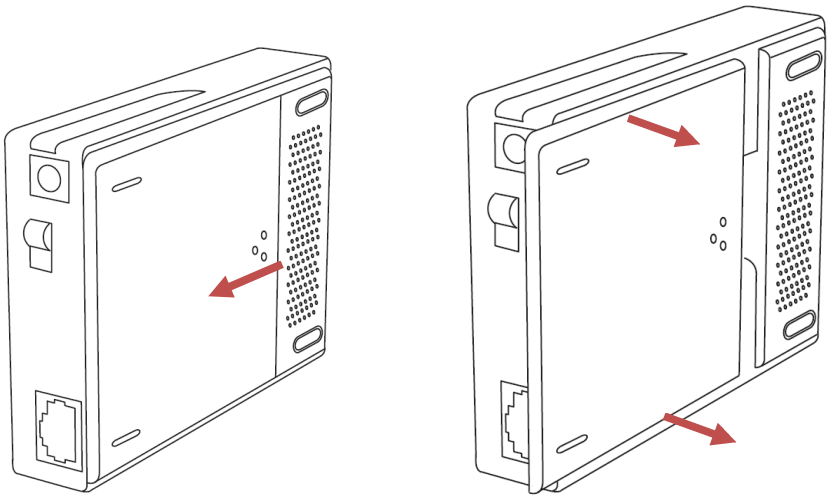
Benefits:

- Works with practically any Wi-Fi enabled device.
- Works with an Ethernet device over a standard RJ45 connector.

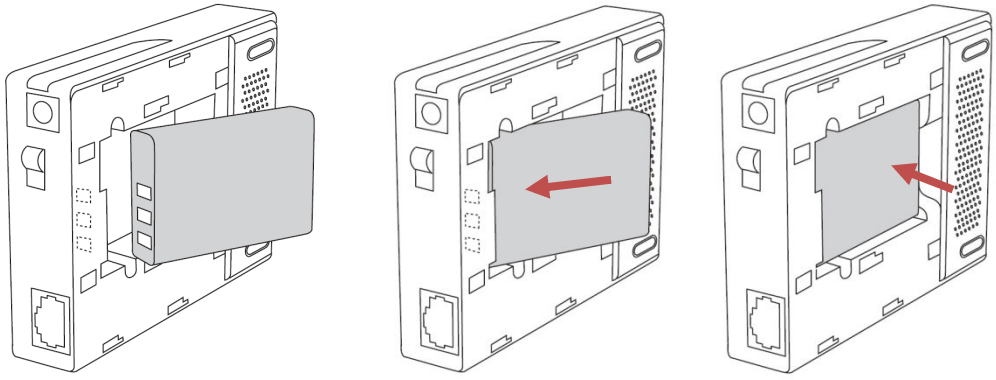
- No need to load software or drivers.
- Shares the Internet connection and links up to 256 devices in a Local Area Network.
- YOYORouter can be located in, for example, a window, providing better signal strength without moving your laptop or other devices.

2.2. Preparing YOYORouter EE1

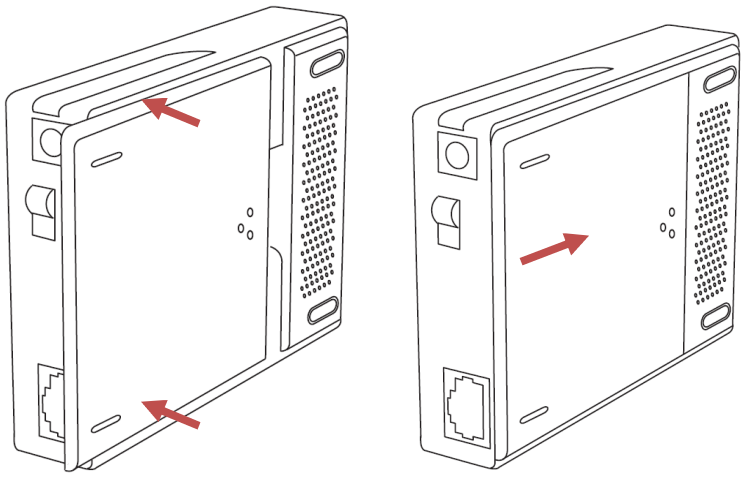
1. Open the battery compartment
   - Slide the cover in the direction shown until it clicks open.
   - Lift the cover away from YOYORouter.



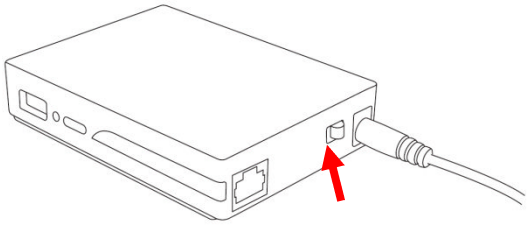
2. Insert the battery
   - **WARNING:** Always be sure to disconnect the power before inserting or removing the battery.
   - Hold the battery so that the three gold contacts align with the three gold pins in the compartment.
   - Insert the battery so that the contacts meet.
   - Press the other end of the battery in to the compartment so that it clips in to place.



3. Replace the battery compartment cover
   - Place the cover over the battery compartment, leaving a gap of about 5mm.
   - Slide the cover towards the body of YOYORouter.
   - The cover clicks shut.



4. Connect the power cord and plug in the AC adaptor.



5. Turn on YOYORouter EE1.

2.3. Connecting to YOYORouter EE1

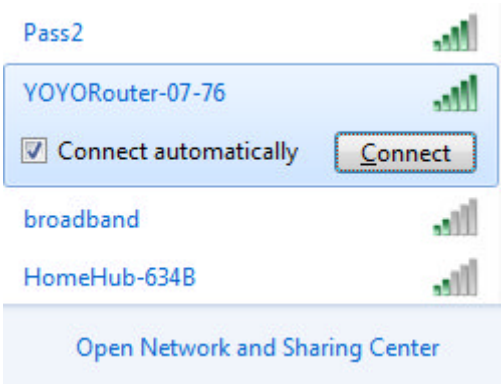
Select YOYORouter's Wi-Fi network which has a network name (SSID) like YOYORouter-07-76. The network name and network password are printed on a label in the battery compartment and on the box.

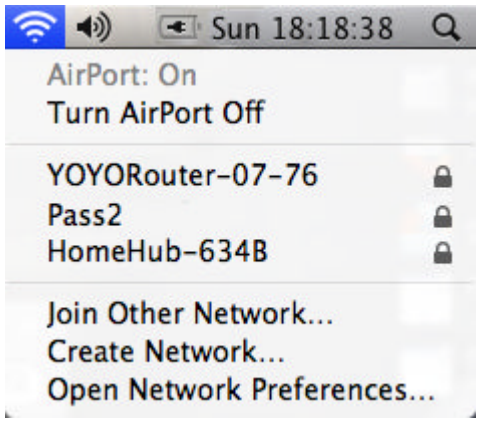
For example, in Windows 7

- Click the icon in the notification area.
- Select your YOYORouter's network.
- Click **Connect** and enter the Wi-Fi password when prompted.

If you are using a Mac

- Click the network icon
- Select your YOYORouter's network.
- When prompted, enter the Wi-Fi password.



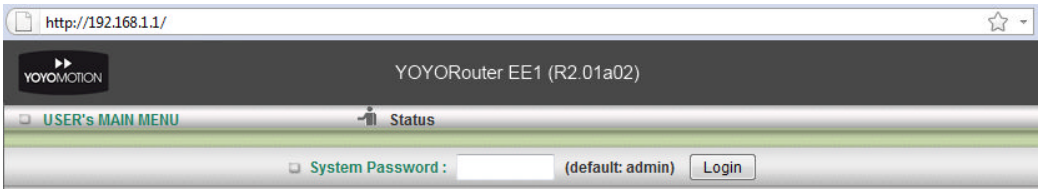


You may also connect using an Ethernet cable, except when YOYORouter is configured in Ethernet WAN Mode, when the Ethernet port is used to connect the WAN.

Note: since connections to YOYORouter are made using Wi-Fi and Ethernet, a wide range of devices including Linux based and mobile can connect without needing any special software or drivers.

2.4. Accessing the status and configuration pages.

1. While connected, open your web browser and enter http://192.168.1.1. The YOYORouter status page is displayed.



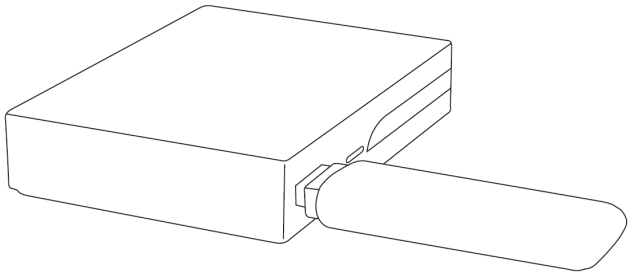
2. To view and change settings, enter the password, default *admin*, and click **Login.**

2.5. Setting up YOYORouter EE1 in Wireless WAN Mode

Note: A full list of supported USB modems is available from the **Supported Cards List** link in the status page, or from www.yoyomotion.com.

1. Make sure your SIM card is installed in the USB modem. Consult the USB Modem's documentation for further information.

2. Plug in your USB Modem and turn on YOYORouter EE1. Allow at least 60 seconds for the USB modem to be detected and configured.



In most cases YOYORouter EE1 self-configures and operates in Wireless WAN Mode using default settings. You may need to customize the settings, for example in the following cases:

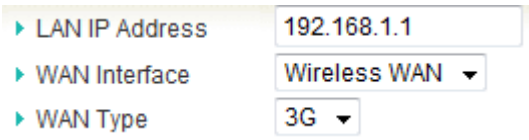
- Your SIM requires a PIN Code.
- Your mobile broadband subscription requires different settings to those that YOYORouter selected by default.
- You have special mobile broadband settings, for example a private APN (Access Point Name).
- You wish to change Wi-Fi settings.

To customize settings:

3. Connect to YOYORouter via Wi-Fi or Ethernet, access the status page at http://192.168.1.1 and log in.

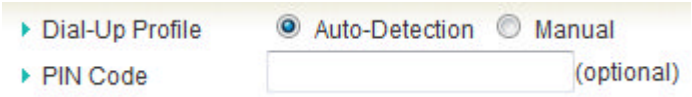
4. Select **Wizard** and step through the Setup wizard until you reach step **Select WAN Type.**

- Select **WAN Interface** option **Wireless WAN.**
- Select **WAN Type 3G.**



5. 3G Mobile Network Settings

- Connection settings are normally selected automatically from your SIM.
- Select **Dial-Up Profile** option **Manual** at the 3G step if you need to select alternative or enter special settings. Select your country and the network operator, or **Others** to enter your own settings.
- If your SIM requires a PIN code, enter it now.



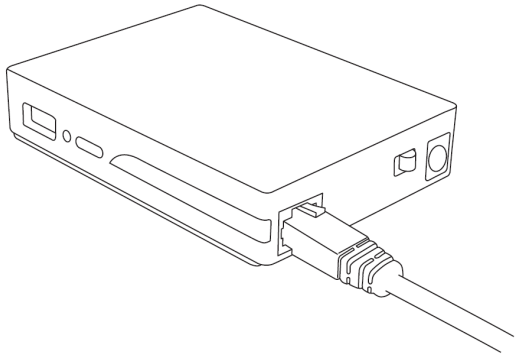
6. At the end of the Wizard, check **The Ethernet Port will be set as LAN Port** and click **Apply Settings**. YOYORouter restarts.

7. If you are connecting using Wi-Fi, you may need to re-make the connection in line with your new settings. If you are using an Ethernet cable, the connection will be active as soon as the reboot is complete.

Note: In this mode you can also connect a device using the Ethernet LAN port. If you do not require the Wi-Fi connection, it may be disabled for longer battery life.

2.6. Setting up YOYORouter EE1 in Ethernet WAN Mode

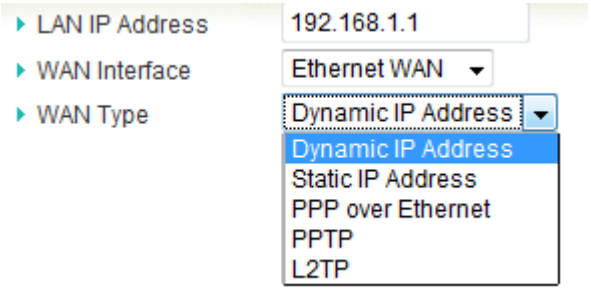
1. Plug in the Ethernet cable and switch on YOYORouter EE1. Typical WAN sources include ADSL modems, cable modems and hotel/office cabled Internet connections.



2. Connect to YOYORouter via Wi-Fi, access the status page at http://192.168.1.1 and log in.

3. Select **Wizard** and step through the Setup wizard. At the step **Select WAN Type**

- Select **WAN Interface** type **Ethernet WAN.**
- Select the required **WAN Type.**
- Enter the further information requested, as applicable. See Configuration Reference section in the User Guide for more information.



4. At the end of the Wizard, check **The Ethernet Port will be set as WAN Port** and click **Apply Settings**. YOYORouter restarts.

5. Re-connect to the YOYORouter Wi-Fi network; you may need to re-make the connection in line with your new settings.

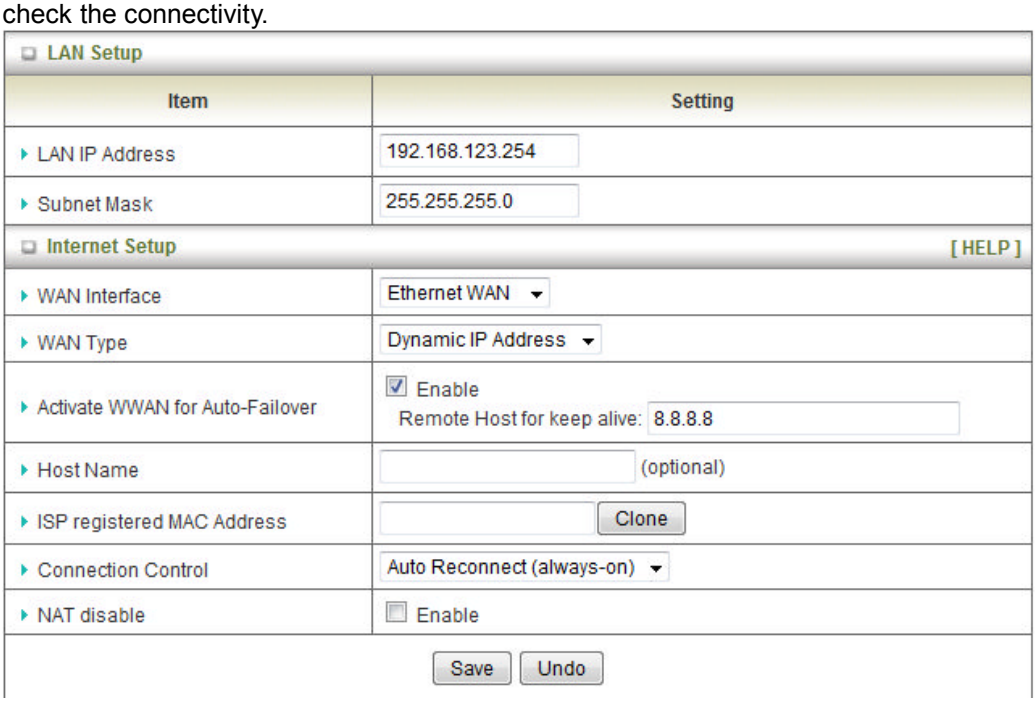
2.7. Setting up YOYORouter EE1 in Ethernet WAN Mode with Failover

First configure YOYORouter EE1 in Wireless WAN Mode and test the connection.

Next, configure YOYORouter EE1 in Cable and test the connection.

To enable WAN Mode with Failover, ensure that the USB Modem and Ethernet WAN are both connected and follow these steps:

1. Log in.
2. Select **Advanced** then **Network Setup.**
3. Against **Activate WWAN for Auto-Failover**
   - Check **Enable**.
   - Enter an IP address in **Remote Host for keep alive** that YOYORouter can ping to check the connectivity.



4. Make sure that **Connection Control** is set to **Auto Reconnect (always on).**
5. Click **Save.**
6. Select **TOOLBOX**, **Reboot** and **OK** to reboot YOYORouter.

7. Check that YOYORouter is normally connected to the cabled WAN connection
   - System Status shows cabled connection details.
   - Wireless Modem indicates Disconnected.

System Status [HELP]

Item	WAN Status	Sidenote
Remaining Lease Time	71:55:42	Renew
IP Address	192.168.0.15	Release
Subnet Mask	255.255.255.0	
Gateway	192.168.0.1	
Domain Name Server	192.168.0.1 , 0.0.0.0	

Wireless Modem Information

Item	Status	Sidenote
Card Info	HSPA USB MODEM	
Link Status	Disconnected.	
Signal Strength	54%	
Network Name	My Operator	

8. Unplug the cabled WAN plug and check that Failover occurs:
   - 3G Failover indicated in System Status.
   - Wireless Modem indicates Connected.

System Status [HELP]

Item	Status	Sidenote
IP Address	10.160.200.219	3G Failover
Subnet Mask	255.255.255.255	
Gateway	10.64.64.64	
Domain Name Server	10.205.65.68 , 10.205.65.68	
Connection Time	00:00:09	

Wireless Modem Information

Item	Status	Sidenote
Card Info	HSPA USB MODEM	
Link Status	Connected.	
Signal Strength	54%	
Network Name	My Operator	

9. Re-connect the cabled WAN and check that service reverts to the WAN connection.

2.8. Setting up YOYORouter EE1 in Share Mode

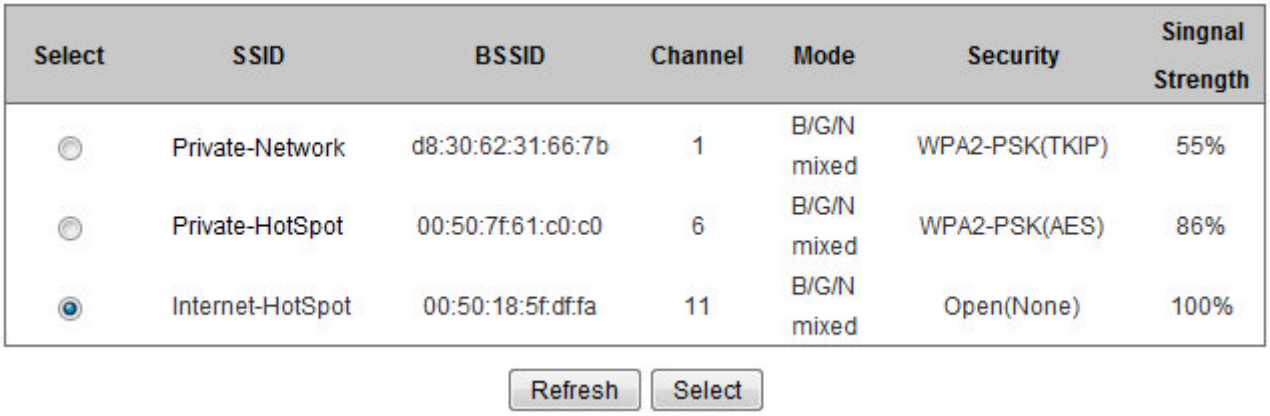
1. Switch on YOYORouter EE1.

2. Connect to YOYORouter via Wi-Fi or Ethernet, access the status page at http://192.168.1.1 and log in.

3. Select **Wizard**. Click through the Wizard making any changes to the default settings if necessary.

4. When you get to **Select WAN Type** in the Wizard
- Select **WAN Interface** to be **Wireless WAN**.
- Select **WAN Type: Wi-Fi HotSpot** and click **Next>**

YOYORouter scans for available Wi-Fi networks and presents a list; select the required network.



Select	SSID	BSSID	Channel	Mode	Security	Singnal Strength
○	Private-Network	d8:30:62:31:66:7b	1	B/G/N mixed	WPA2-PSK(TKIP)	55%
○	Private-HotSpot	00:50:7f:61:c0:c0	6	B/G/N mixed	WPA2-PSK(AES)	86%
◉	Internet-HotSpot	00:50:18:5f:df:fa	11	B/G/N mixed	Open(None)	100%

Refresh Select

5. Enter any required security details for the Wi-Fi network to which you are connecting. The YOYORouter automatically uses the same Wireless Channel.

6. At the end of the Wizard, check **The Ethernet will be set as LAN Port** and click **Apply Settings**. YOYORouter restarts.

7. Re-connect to the YOYORouter Wi-Fi network; you may need to re-make the connection in line with your new settings.

8. If the Wi-Fi network to which you are connecting requires a username and password at a log-in page, open your browser and input them now.

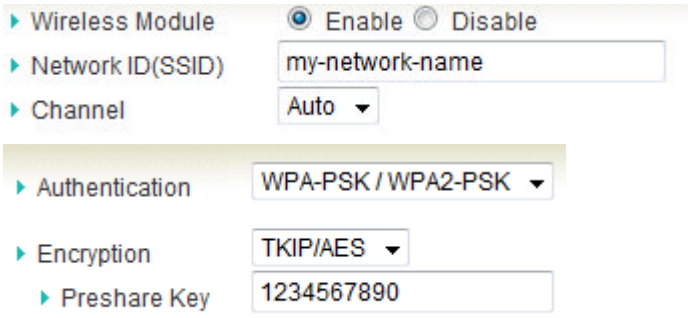
Note: In this mode you can also connect a device using the Ethernet LAN port.

2.9. Wi-Fi Configuration Tips

YOYORouter is pre-configured with a default Wi-Fi network name (SSID) and password. The network name and password are printed on the label on the underside of the device and on the label affixed to the carton in which it was packaged. Security is set to WPA-PSK(TKIP) and WPA2-PSK(AES) – devices may connect using either of these.

In the Configuration Wizard you can:

- Change the Network ID (SSID) to a name of your own choice.
- Manually select a frequency channel. (Default **Auto** tries to find a channel with low interference).
- Change the Authentication and Encryption settings if required.
- Set your own network password in **Preshare Key** (recommended).



2.10. Connecting to the YOYORouter using WPS

Wi-Fi Protected Setup, WPS, is a simple way to connect to the YOYORouter without needing to give the new user the Pre-Shared Key (password). Pushbutton mode provides the simplest possible configuration:

1. Locate the WPS pushbutton on the device that you wish to connect to the router. This may be a physical button or a clickable pushbutton in the software provided with the device.
2. Press and hold the YOYORouter WPS button for 5 seconds. The Wi-Fi indicator will flash rapidly
3. Bring the device near to the YOYORouter and press the WPS button on the device. You must do this inside two minutes, while the Wi-Fi indicator flashes rapidly. The GUI on the connecting device will confirm the connection.

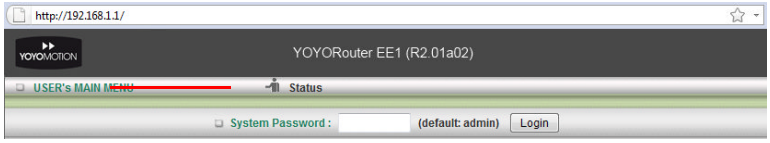
PIN Mode is also supported.

3. Configuration Reference Guide

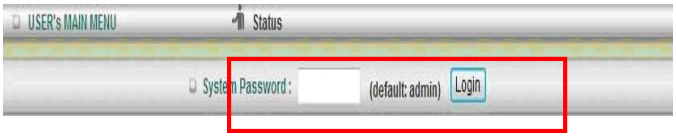
3.1. Using the Setup Wizard

3.1.1. Starting the Wizard

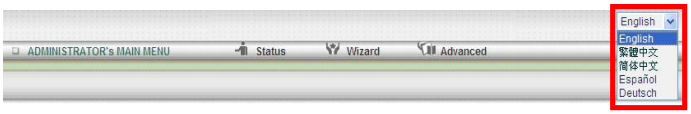
Please type in the IP Address (http://192.168.1.1)

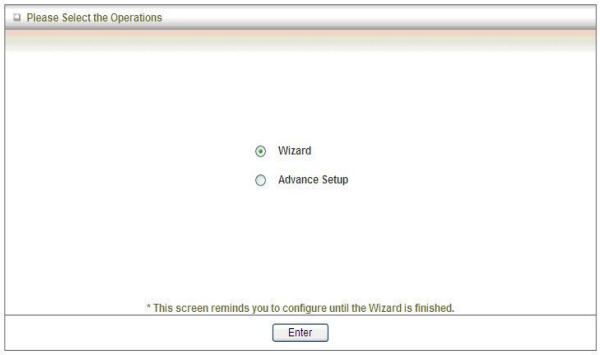


Please type “admin” in the Password and click the **Login** button.



Select your language.




Please Select the Operations
Wizard
Advance Setup
* This screen reminds you to configure until the Wizard is finished.
Enter

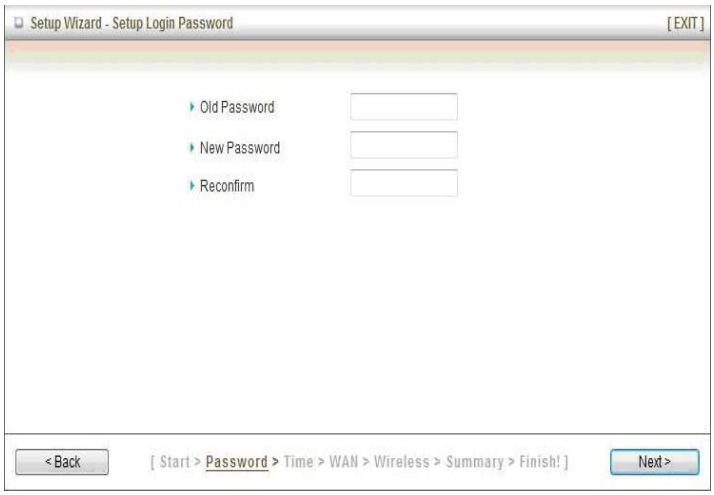
Press “Next” to start the Setup Wizard.

Setup Wizard
[EXIT]
Setup Wizard will guide you through a basic configuration procedure step by step.
Step 1. Setup Login Password.
Step 2. WAN Setup.
Step 3. Wireless Setup.
Step 4. Summary.
Step 5. Finish.
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

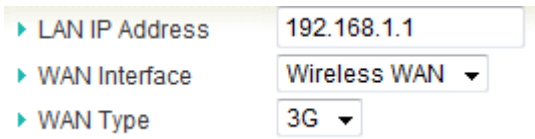
3.1.2. Configure Settings using the Wizard

Step 1.
Change System Password.

Set up your system password.
(Default：admin)

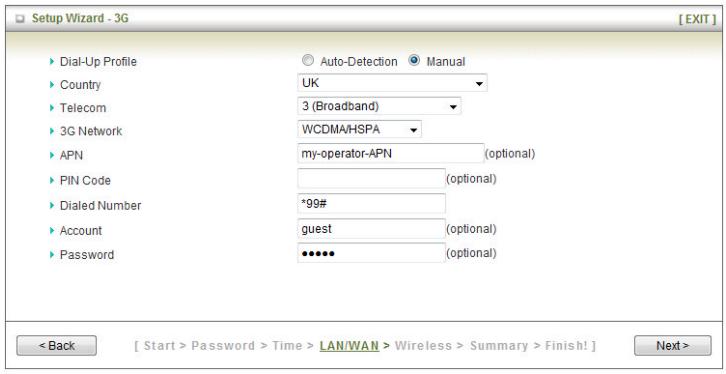

Setup Wizard - Setup Login Password
[EXIT]
Old Password
New Password
Reconfirm
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

Step 2a.
Select LAN IP Address and Wan Type.



Step 2b.
3G WAN type
Select “Auto Detection” Dial-up Profile, and the Utility will try to detect and configure the required Mobile Broadband service settings automatically. Or you can select “Manual” and select your country and mobile operator. If you have special settings, for example for a private company, select your country and then **Others.**

If your SIM card requires a PIN Code, enter it, otherwise leave blank.



Step 3a.

Set up your Wireless Network.

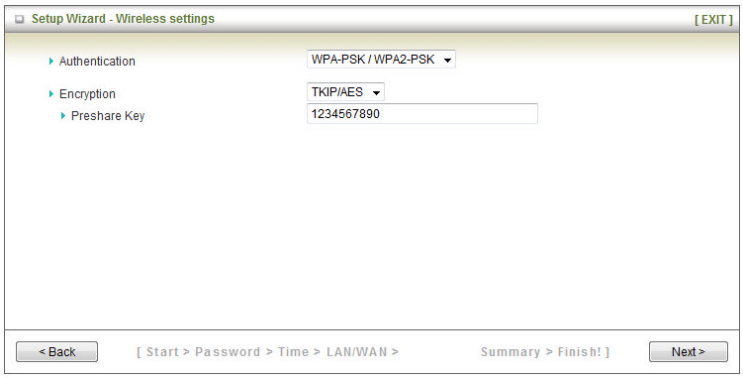
Set up your Wi-Fi network name (SSID).

Channel **Auto** (default enables the router to identify the best channel. If you wish to manually select the channel, typically 1, 6 or 11, pick it in the drop-down menu.

Step 3b.

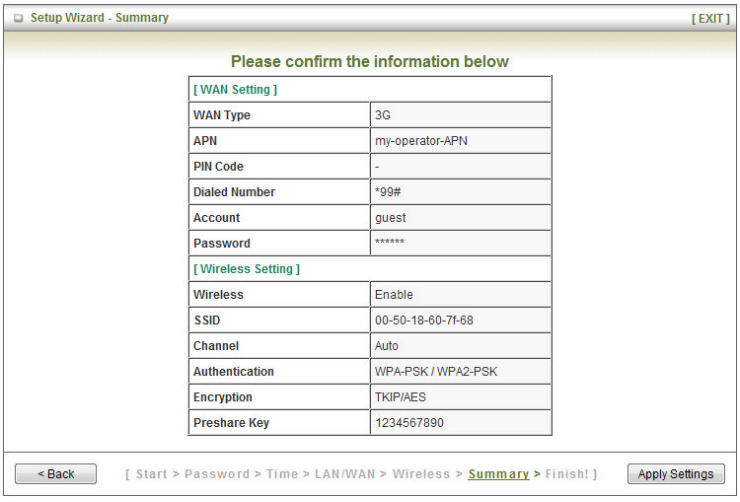
Set up Wireless Security.

We recommend WPA-PSK / WPA2-PSK security. The settings shown provide widest compatibility.You can set your own password in **Preshare Key**.

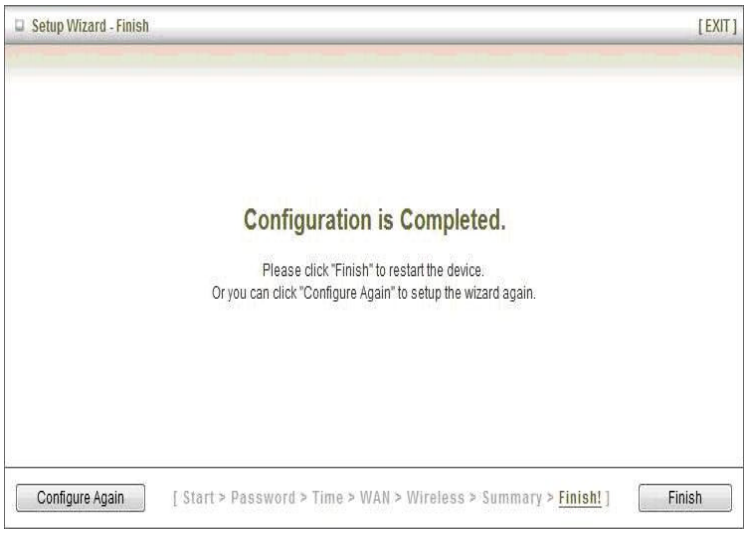


Step 4.

The settings you have selected are summarized. Click **Apply Settings** to confirm them.
The wizard counts down the time it takes while YOYORouter re-starts.



Step 5.
Click Finish to close the Wizard.
Note: The router has already restarted.


Setup Wizard - Finish
[EXIT]
Configuration is Completed.
Please click "Finish" to restart the device.
Or you can click "Configure Again" to setup the wizard again.
Configure Again
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Finish

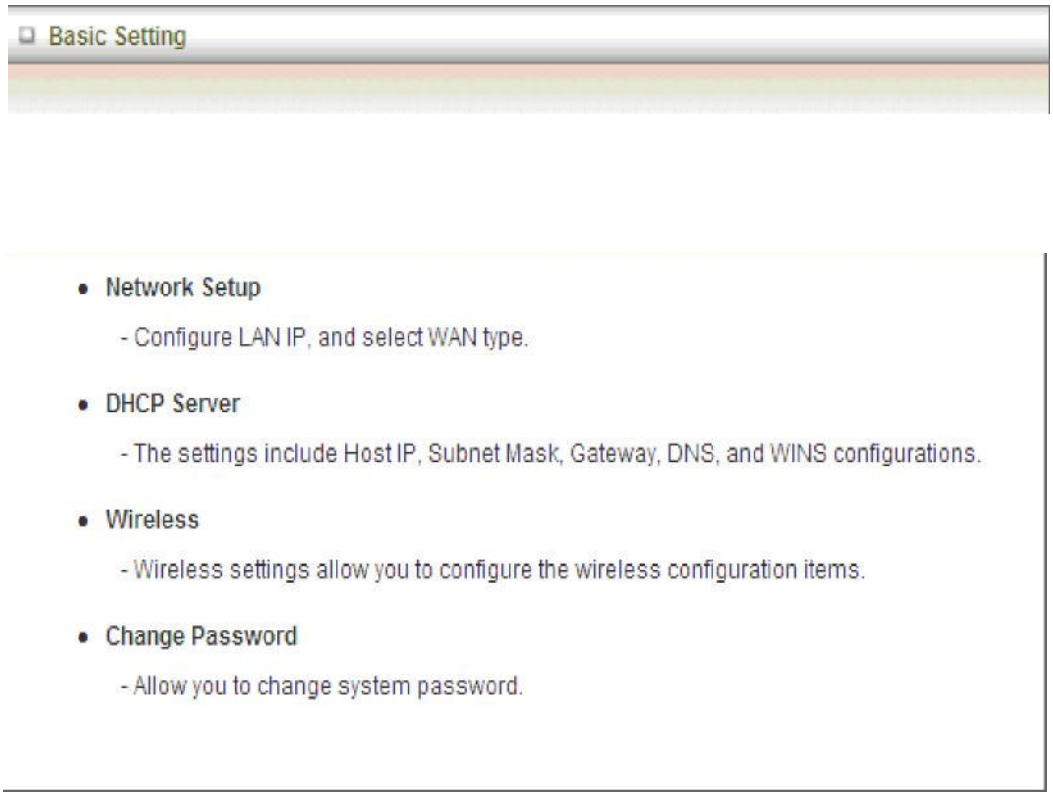
3.2. Advanced Settings

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the device. The default IP Address is: 192.168.1.1

Enter the default password “admin” in the System Password and then click ‘login’ button.

Then, you can browse the “Advanced” configuration pages for configuring this device.

3.2.1. Basic Setting Group


Basic Setting
Network Setup
- Configure LAN IP, and select WAN type.
DHCP Server
- The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
Wireless
- Wireless settings allow you to configure the wireless configuration items.
Change Password
- Allow you to change system password.

3.2.1.1. Network Setup

1. **Ethernet port Configuration:**

   Off: Disable the Ethernet port.

   LAN: The Ethernet port is as LAN port.

   WAN: The Ethernet port is as LAN port.

   Auto: It will be WAN Port if a DHCP server can be detected on the Ethernet port. Otherwise, it will be LAN port.

2. **LAN IP Address:** The local IP address of this device. The computers on your network must use the LAN IP address of this device as their Default Router. You can change it if necessary.

3. **Subnet Mask:** Input your Subnet mask. (All devices in the network must have the same subnet mask.) The default subnet mask is 255.255.255.0.

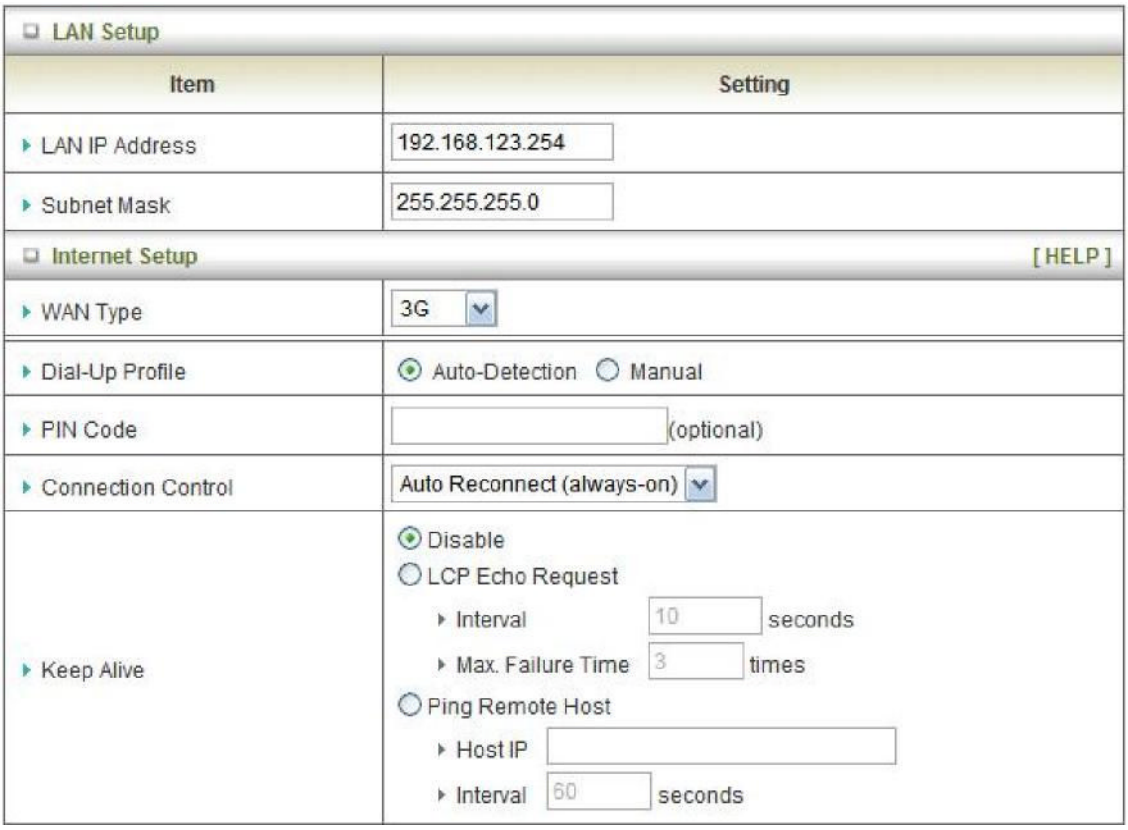
4. **WAN Interface:** Select Ethernet WAN or Wireless WAN to continue.

5. **WAN Type**: WAN connection type of your ISP. You can click WAN Type combo button to choose a correct one from the following options:

A. 3G

This device supports different WAN types of connection for users to connect to remote wireless ISP, such as 3G (WCDMA, HSxPA, HSPA+, CDMA2000, EV-DO, TD-SCDMA), iBurst, or Wi-Fi Hotspot.

Note. Users need to insert USB modem card for 3G and iBurst WAN connections.



3G WAN Types: The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect with the 3G network.

Please refer to your documentation or service provider for additional information.

1. Dial-Up Profile: Please select Auto-Detection or Manual to continue.

   You can Select “Auto-Detection”, and the Utility will try to detect and configure the required 3G service settings automatically. Or you can select “Manual” and manually fill in the required 3G service settings provided by your ISP.
2. Country: select your country.
3. Telecom: select your telecom.
4. 3G Network: select the 3G Network
5. APN: Enter the APN for your PC card here.(Optional)
6. Pin Code: Enter the Pin Code for your SIM card(Optional)
7. Dial-Number: This field should not be altered except when required by your service provider.

8. Account: Enter the new User Name for your PC card here, you can contact to your ISP to get it.
9. Password: Enter the new Password for your PC card here, you can contact to your ISP to get it.
10. Authentication: Choose your authentication.
11. Primary DNS: This feature allows you to assign a Primary DNS Server, contact to your ISP to get it.
12. Secondary DNS: This feature allows you to assign a Secondary DNS Server, you can contact to your ISP to get it.
13. Connection Control: There are 3 modes to select:

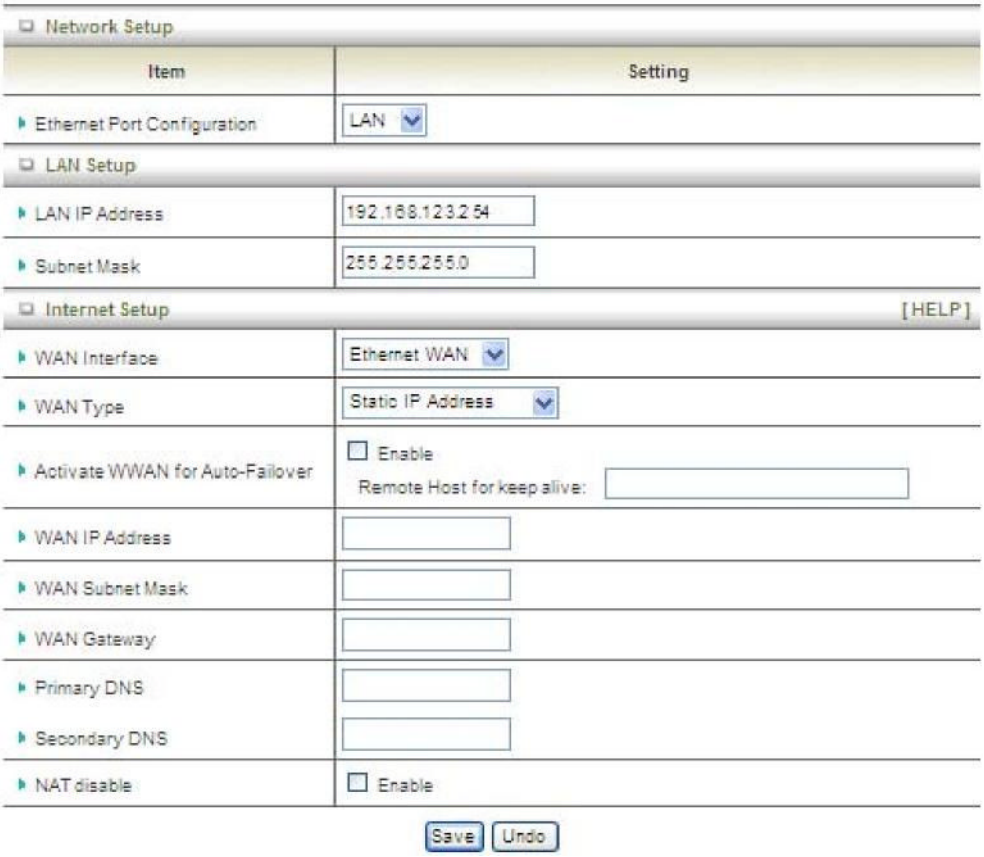
    Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

    Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

    Manually: The device will not make the link until someone clicks the Connect-button in the Status-page.
14. Keep Alive: you can diagnose your connection by it.

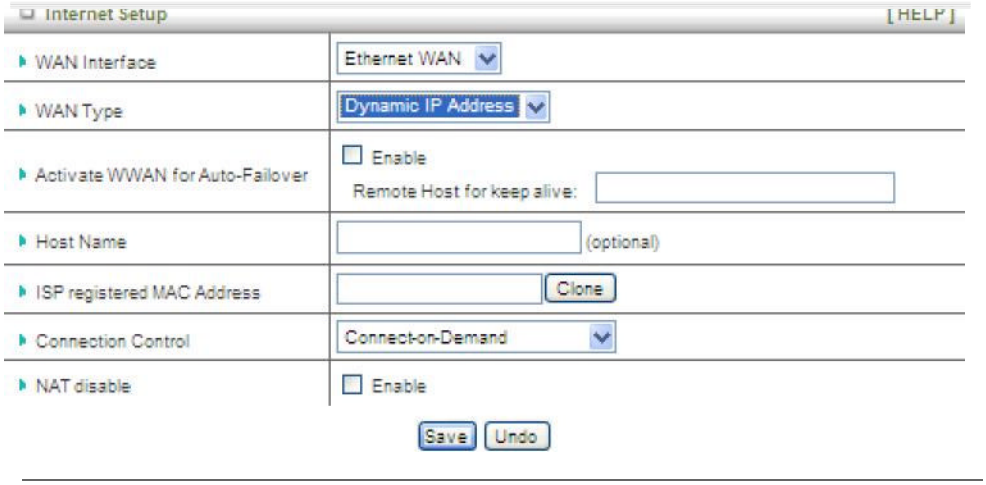
LCP Echo Request: Enter the time interval and the maximum failure count. The device will constantly send out the LCP packets for keeping the connection alive.
Ping Remote Host: Enter the Remote host IP and the time interval to send the ping packets for keeping the connection alive.

B. Static IP Address:



1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service.
2. **WAN IP Address, Subnet Mask, Router, Primary and Secondary DNS**: Enter the proper settings provided by your ISP.

C. Dynamic IP Address:



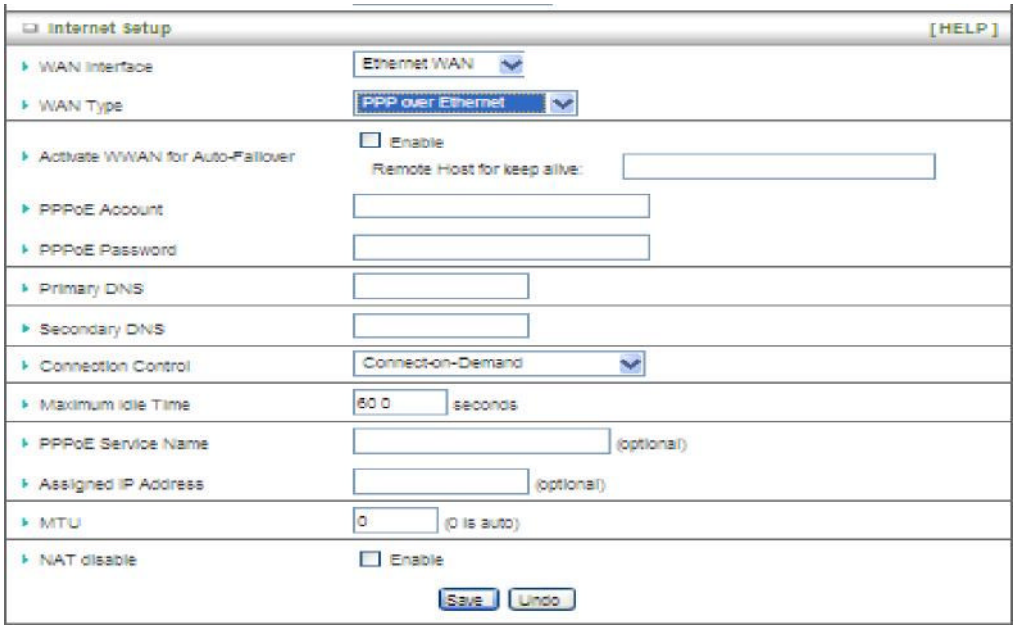
1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service
2. **Host Name**: Optional, required by some ISPs, for example, @Home.
3. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

D. PPP over Ethernet



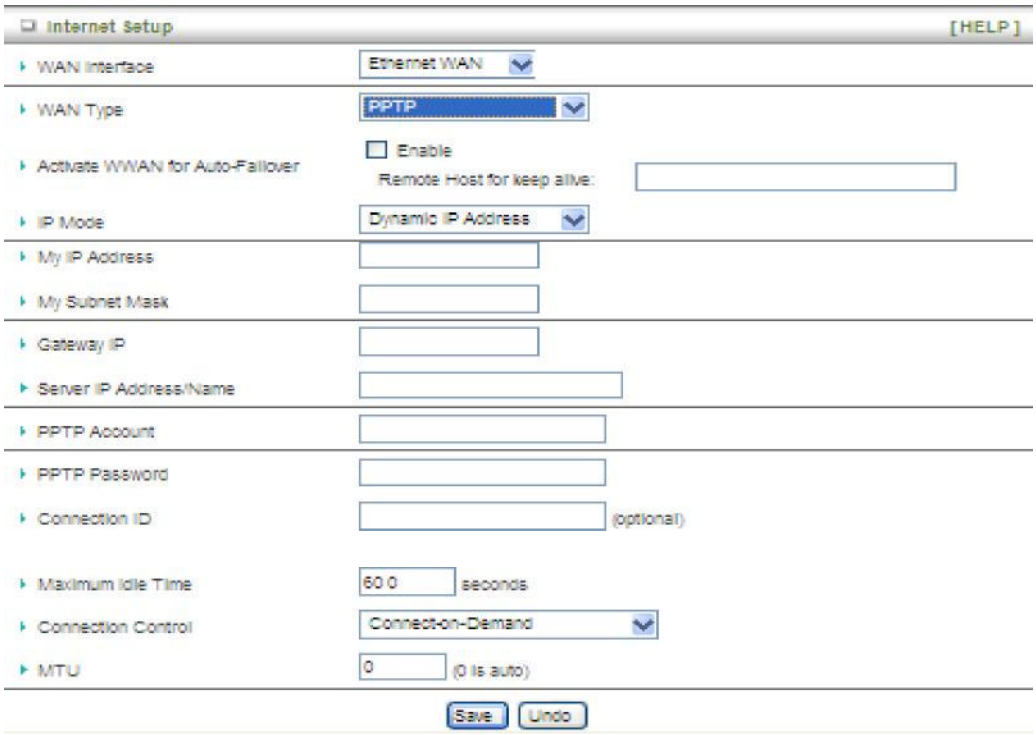
1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service
2. **PPPoE Account** and **Password**: The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
3. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
4. **Maximum Idle Time**: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable "Auto-reconnect" to disable this feature.
5. **PPPoE Service Name**: Optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
6. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).

E. PPTP



1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service
2. **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address”.
3. **My IP Address** and **My Subnet Mask**: The private IP address and subnet mask your ISP assigned to you.
4. **Router IP** and **Server IP Address/Name**: The IP address of the PPTP server and designated Router provided by your ISP.
5. **PPTP Account** and **Password**: The account and password your ISP assigned to you. If you don't want to change the password, keep it blank.
6. **Connection ID**: Optional. Input the connection ID if your ISP requires it.
7. **Maximum Idle Time**: the time of no activity to disconnect your PPTP session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this device will connect with ISP automatically after system is restarted or connection is dropped.
8. **Connection Control**: There are 3 modes to select:

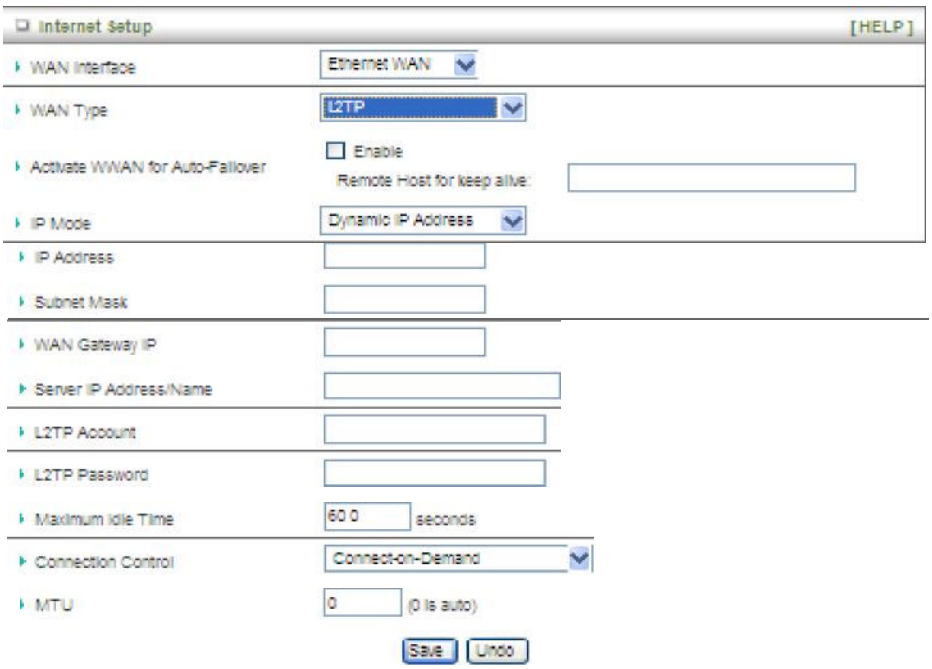
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

9. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default MTU value is 0 (auto).

F. L2TP



1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service
2. **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address”.
3. **My IP Address** and **My Subnet Mask**: The private IP address and subnet mask your ISP assigned to you.
4. **Router IP** and **Server IP Address/Name**: The IP address of the L2TP server and designated Router provided by your ISP.
5. **L2TP Account** and **Password**: The account and password your ISP assigned to you. If you don't want to change the password, keep it blank.
6. **Connection ID**: Optional. Input the connection ID if your ISP requires it.

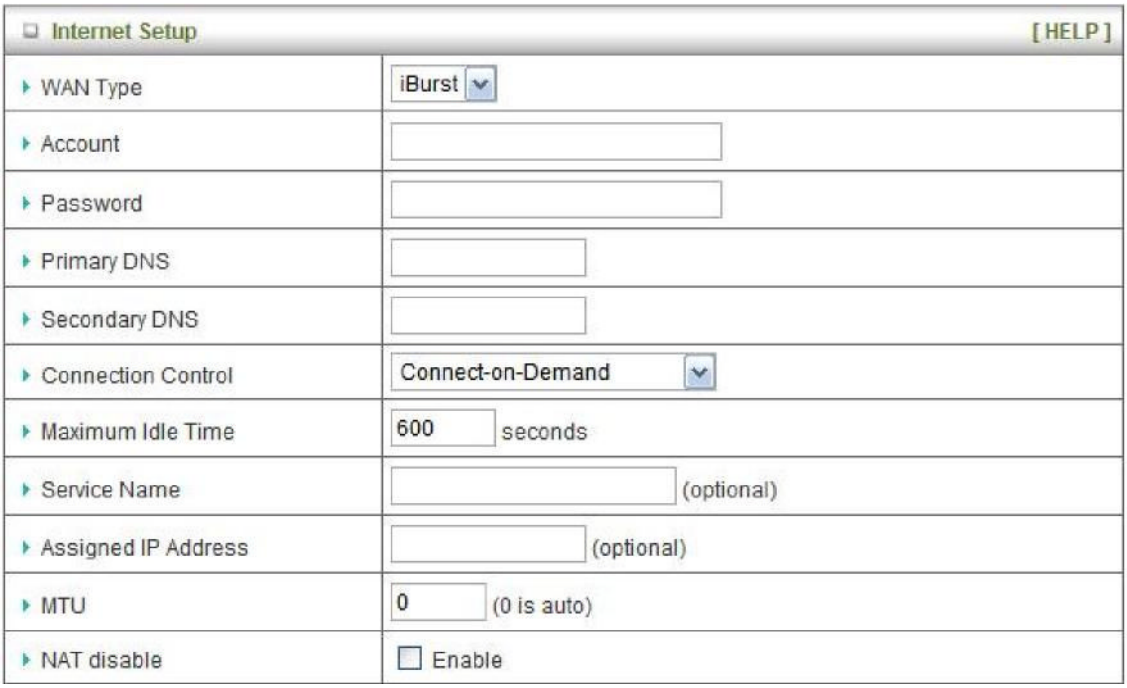
7. **Maximum Idle Time**: The time of no activity to disconnect your L2TP session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this device will connect with ISP automatically, after system is restarted or connection is dropped.
8. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
9. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default MTU value is 0 (auto).

G. iBurst



iBurst Type: The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect with the iBurst network.

Please refer to your documentation or service provider for additional information.

1. Account: Enter the new User Name for your PC card here, you can contact to your ISP to get it.
2. Password: Enter the new Password for your PC card here, you can contact to your ISP to get it.

3. Primary DNS/Secondary DNS: Optional, This feature allows you to assign a DNS Servers
4. Connection Control: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

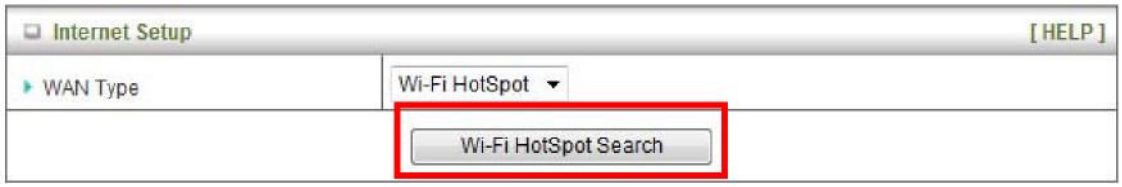
   Manually: The device will not make the link until someone clicks the Connect-button in the Status-page.
5. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable "Auto-reconnect" to disable this feature.
6. Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
7. Assigned IP Address: Optional, Input the IF address you want. Usually, leave it blank.
8. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).
9. NAT disable: the option bridges data form WAN port to LAN port.

H. **Wi-Fi HotSpot**

Wi-Fi HotSpot Types: This WAN type allows you to share one Wi-Fi Hotspot account with your friends or colleagues. Local clients connect to this device via Wi-Fi connection, and surfing Internet by connecting to remote Wi-Fi Hotspot. Just follow a few steps below to connect to remote Wi-Fi HotSpot.

Note. If choosing Wi-Fi HotSpot WAN type, the wireless channel of WLAN will be set to as same as wireless channel of remote Wi-Fi HotSpot.

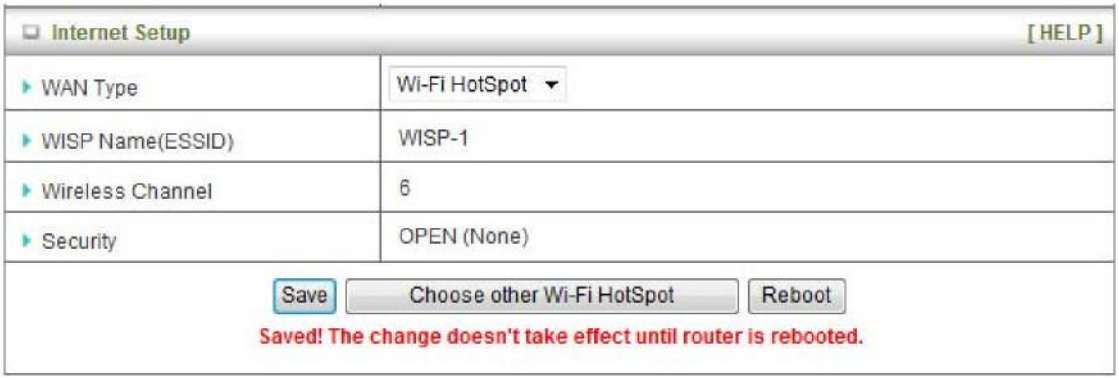
Step 1: Click “Wi-Fi HotSpot” Search” button to search any available Wi-Fi Hotspot or Wi-Fi AP (Access Point) in your environment.



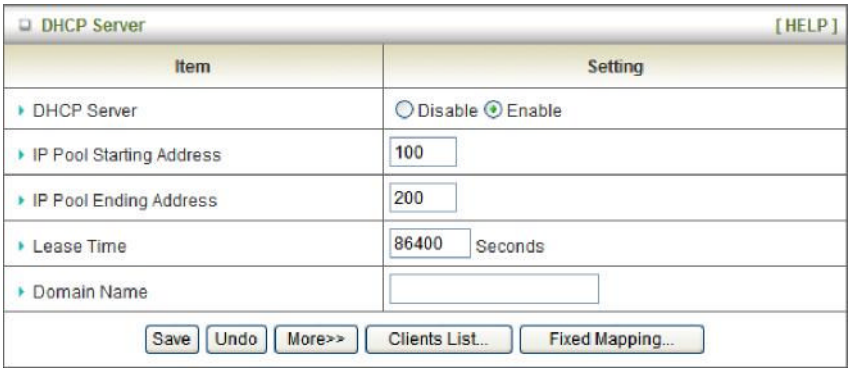
Step 2: After finish searching, it will list all available Wi-Fi APs in your environment. You can select one of the lists to start to connect, or press “Refresh” button to search again.

Step 3: Click “Save” button to save settings after selecting. There will be a field here for you to input encryption key if remote Wi-Fi Hotspot or Wi-Fi AP requires.

Step 4: Click “Reboot” button to restart device to take new settings effective.



3.2.1.2. DHCP Server

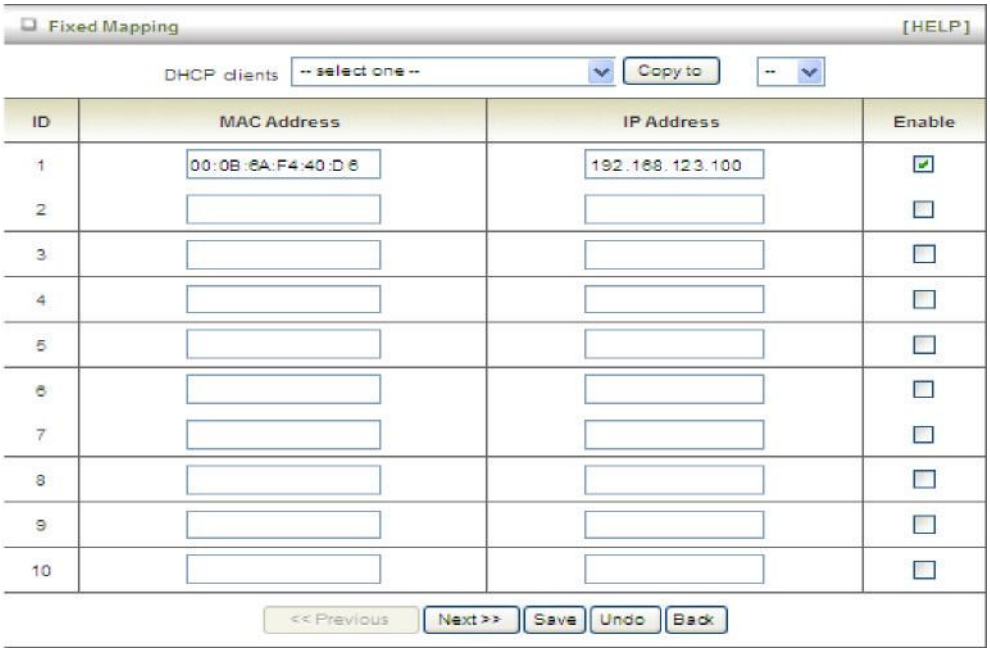


1. **DHCP Server:** Choose either **Disable** or **Enable**. If you enable the DHCP Server function, the following settings will be effective.
2. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool.
3. **Lease Time:** DHCP lease time to the DHCP client.
4. **Domain Name:** Optional, this information will be passed to the clients.
   Press **"More>>"** and you can find more settings
5. **Primary DNS/Secondary DNS:** Optional. This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign a WINS Servers
7. **Router:** Optional. Router Address would be the IP address of an alternate Router. This function enables you to assign another Router to your PC, when DHCP server offers an IP to your PC.

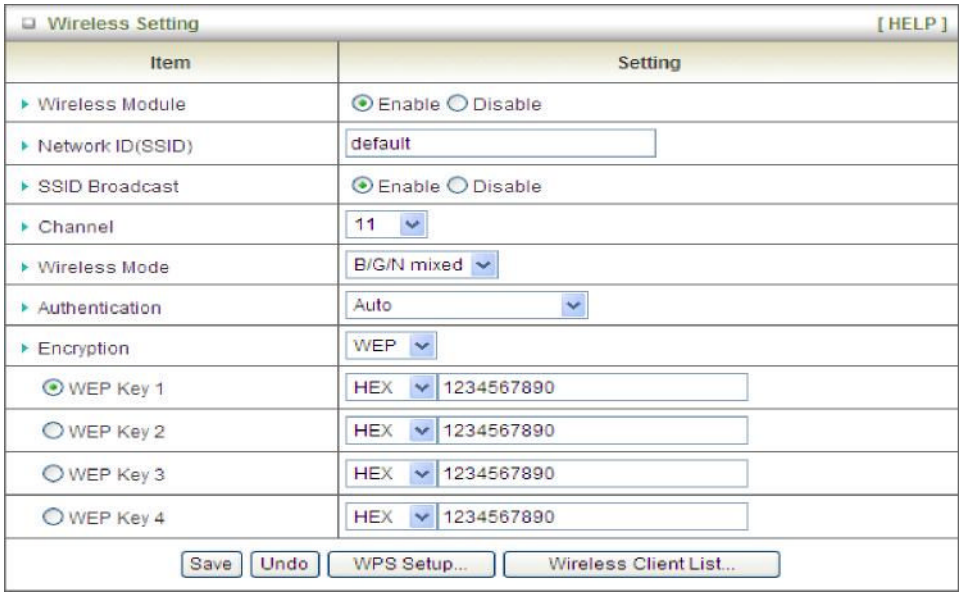
Click on "Save" to store your settings or click "Undo" to give up the changes.

Press "Clients List" and the list of DHCP clients will be shown consequently.

Press “Fixed Mapping” and the DHCP Server will reserve the special IP for designated MAC address.



3.2.1.3. Wireless Settings



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module:** You can enable or disable wireless function.
2. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
3. **SSID Broadcast:** The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
4. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is as follow: channel 1~11 for North America. (Channel 1~13 for European (ETSI); channel1~ 14 for Japan).
5. **Wireless Mode:** Choose “B/G mixed”, “B only”, “G only”, “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
6. **Authentication mode:** You may select one of authentication to secure your wireless network: Open Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

Open

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

Shared

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

Auto

The AP will Select the Open or Shared by the client's request automatically.

WPA-PSK

Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits. If you select ASCII, the length of pre-share key is from 8 to 63.

Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits If you select ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK2

WPA-PSK2 user AES and TKIP for Same the encryption, the others are same the WPA-PSK.

WPA2

WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

WPA-PSK/WPA-PSK2

Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

WPA/WPA2

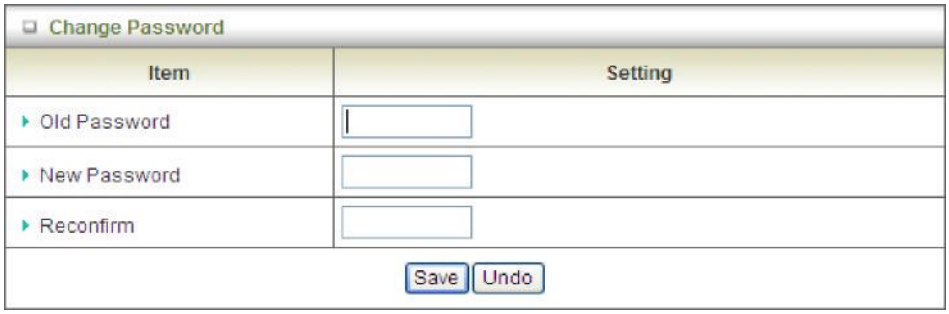
Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

By pressing **"WPS Setup"**, you can configure and enable the easy setup feature WPS (Wi-Fi Protection Setup) for your wireless network.

1. **WPS:** You can enable this function by selecting "Enable". WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
2. **AP PIN**: You can press Generate New Pin to get an AP PIN.
3. **Config Mode**: Select your config Mode from "Registrar" or "Enrollee".
4. **Config Status**: It shows the status of your configuration.
5. **Config Method**: You can select the Config Method here from "Pin Code" or "Push Button".
6. **WPS status**: According to your setting, the status will show "Start Process" or "No used"

Press "Wireless Clients List" and the list of wireless clients will be shown consequently.

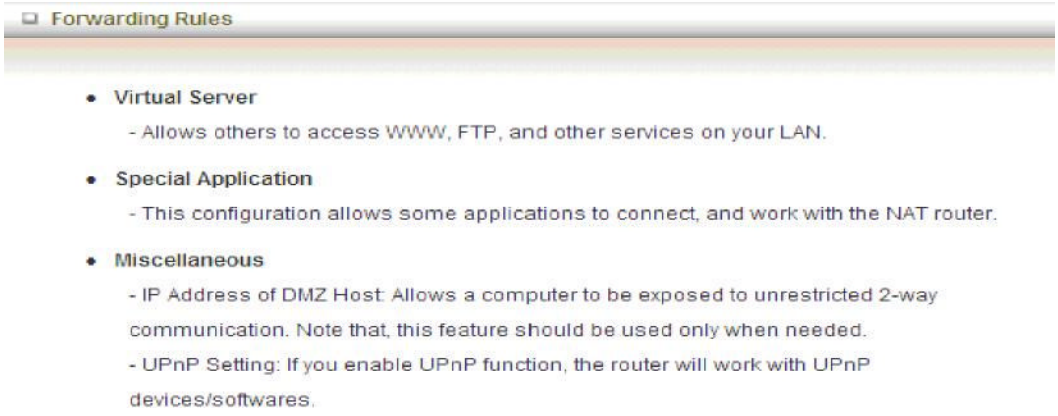
3.2.1.4. Change Password



You can change the System Password here. We **strongly** recommend you to change the system password for security reason.

Click on "Save" to store your settings or click "Undo" to give up the changes.

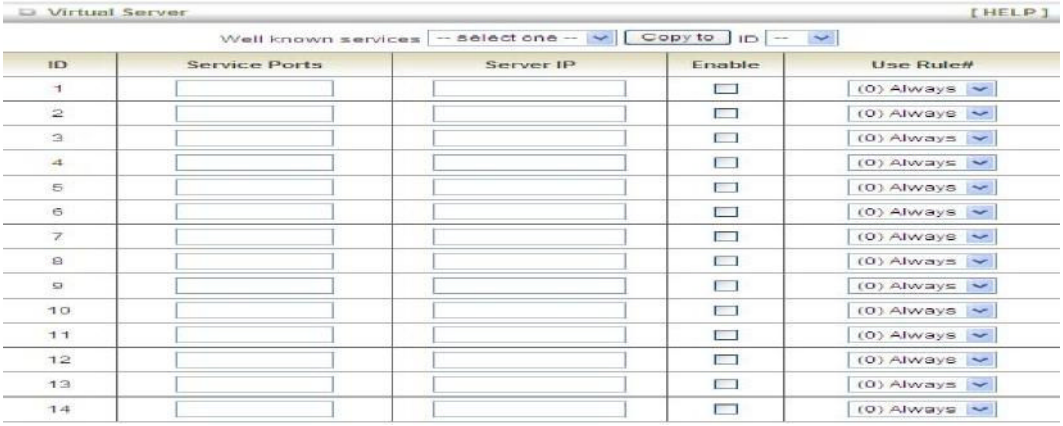
3.2.2. Forwarding Rules


Forwarding Rules
Virtual Server
- Allows others to access WWW, FTP, and other services on your LAN.
Special Application
- This configuration allows some applications to connect, and work with the NAT router.
Miscellaneous
- IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
- UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/softwares.

3.2.2.1. Virtual Server

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP. Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For the details, please refer to **Scheduling Rule**.


Virtual Server
[HELP]
Well known services -- select one -- Copy to ID --
ID
Service Ports
Server IP
Enable
Use Rule#
1 2 3 4 5 6 7 8 9 10 11 12 13 14
(0) Always

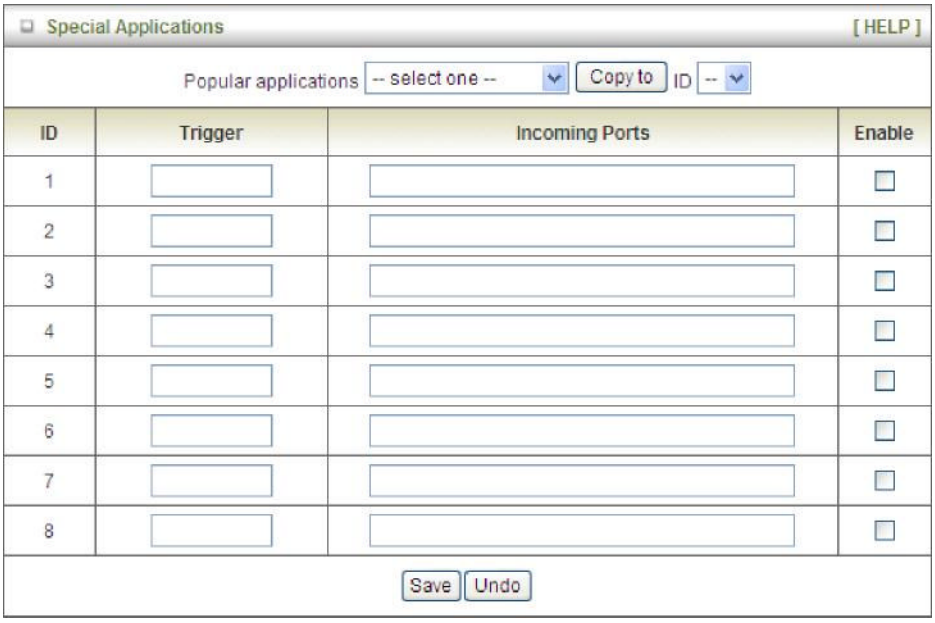
For example, if you have an FTP server (port 21) at 192.168.1.1, a Web server (port 80) at 192.168.1.2, and a VPN server at 192.168.1.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.1.1	V
80	192.168.1.2	V
1723	192.168.1.6	V

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.2.2. Special AP

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

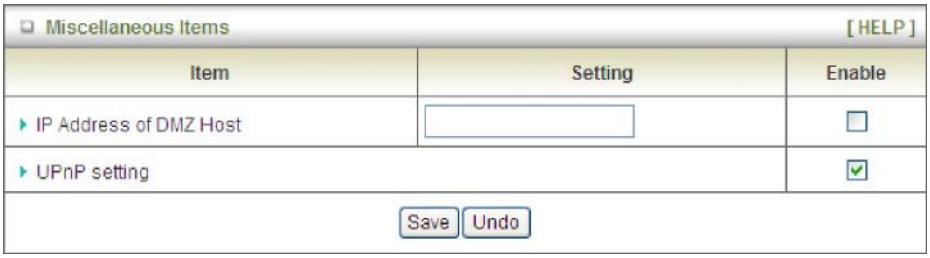


1. **Trigger:** The outbound port number issued by the application.
2. **Incoming Ports**: When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This device provides some predefined settings. Select your application and click "**Copy to**" to add the predefined setting to your list.

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.2.3. Miscellaneous



1. **IP Address of DMZ Host**

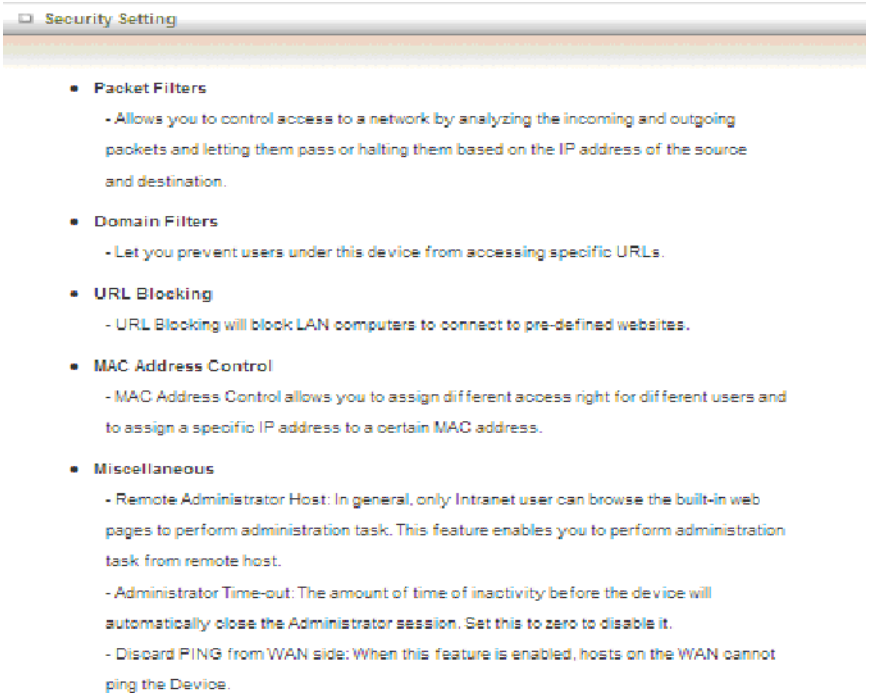
   DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

2. **UPnP Setting**

   The device supports the UPnP function. If the OS of your client computer supports this function, and you enabled it, like Windows XP, you can see the following icon when the client computer gets IP from the device.

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.3. Security Setting

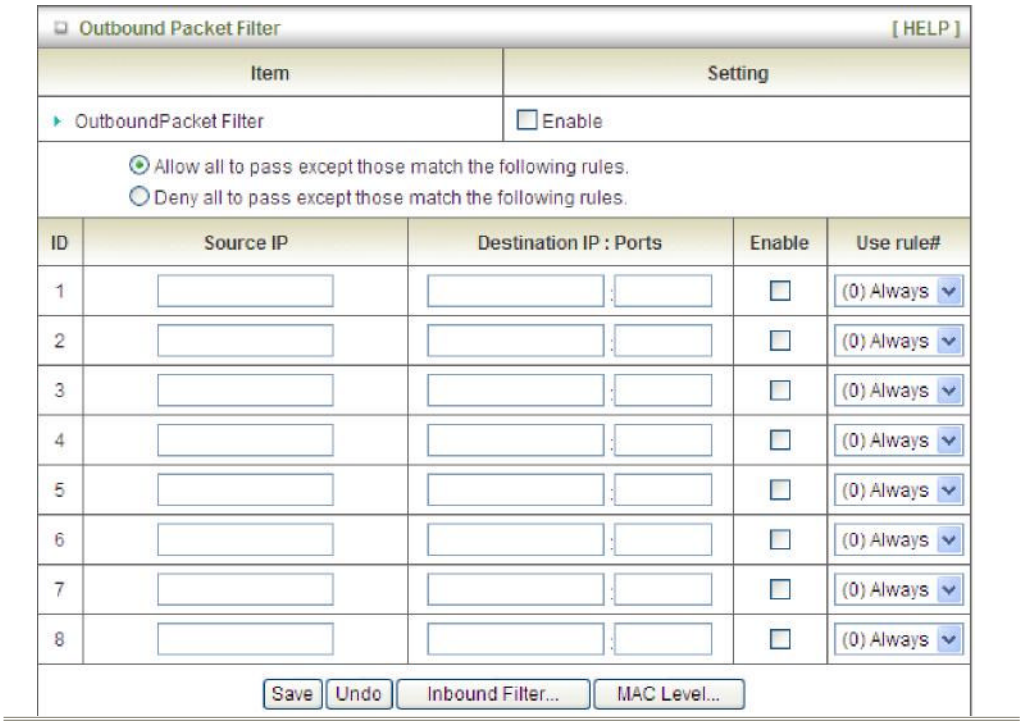

Security Setting
Packet Filters
- Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
Domain Filters
- Let you prevent users under this device from accessing specific URLs.
URL Blocking
- URL Blocking will block LAN computers to connect to pre-defined websites.
MAC Address Control
- MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
Miscellaneous
- Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
- Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
- Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

3.2.3.1. Packet Filters

Packet Filter includes both outbound filter and inbound filter. And they have same way to setting.

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules



You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

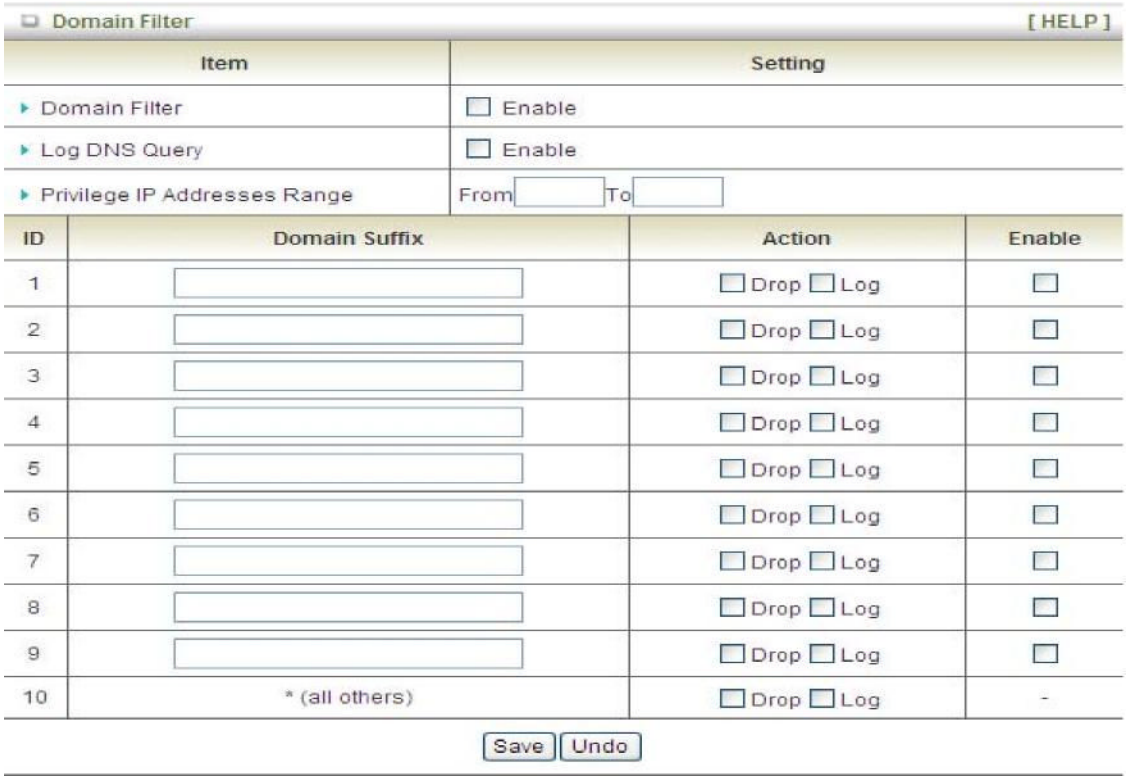
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules,** and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule.**

Each rule can be enabled or disabled individually.

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.3.2. Domain Filters



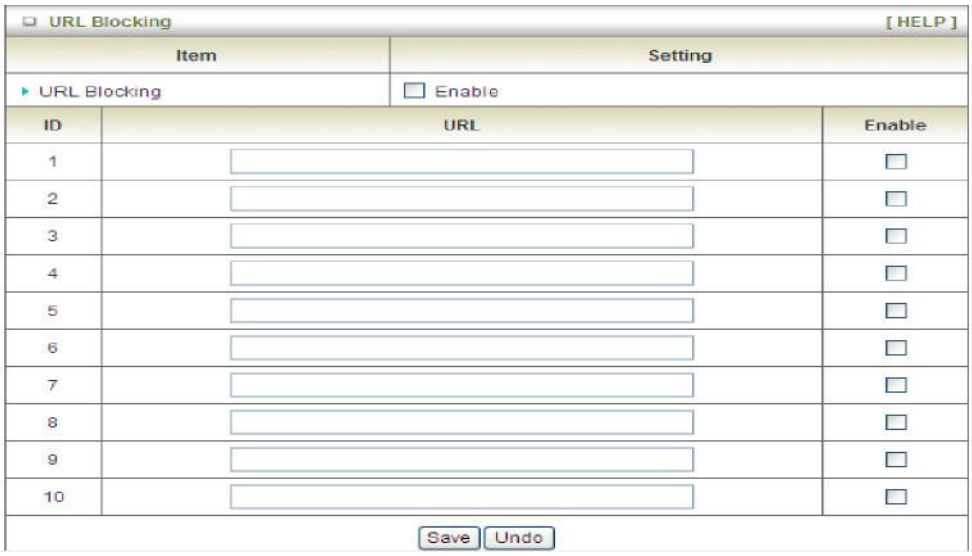
Domain Filter prevents users under this device from accessing specific URLs.

1. **Domain Filter**: Check if you want to enable Domain Filter.
2. **Log DNS Query**: Check if you want to log the action when someone accesses the specific URLs.
3. **Privilege IP Address Range**: Setting a group of hosts and privilege these hosts to access network without restriction.
4. **Domain Suffix**: A suffix of URL can be restricted, for example, ".com", "xxx.com".
5. **Action**: When someone is accessing the URL met the domain-suffix, what kind of action you want.
   Check "Drop" to block the access. Check "Log" to log this access.
6. **Enable**: Check to enable each rule. **Click on "Save" to store your settings**

or click "Undo" to give up the changes.

3.2.3.3. URL Blocking

URL Blocking will block LAN computers to connect with pre-define Websites. The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.



1. **URL Blocking**: Check if you want to enable URL Blocking.
2. **URL**: If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

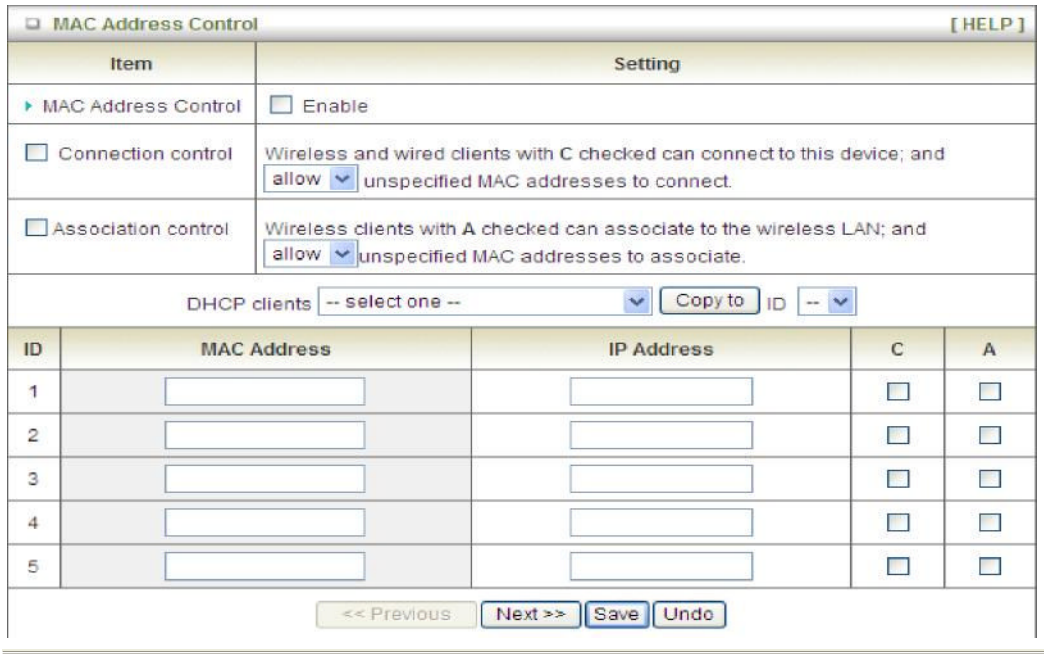
   For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

3. **Enable**: Check to enable each rule.

Click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.3.4. MAC Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.



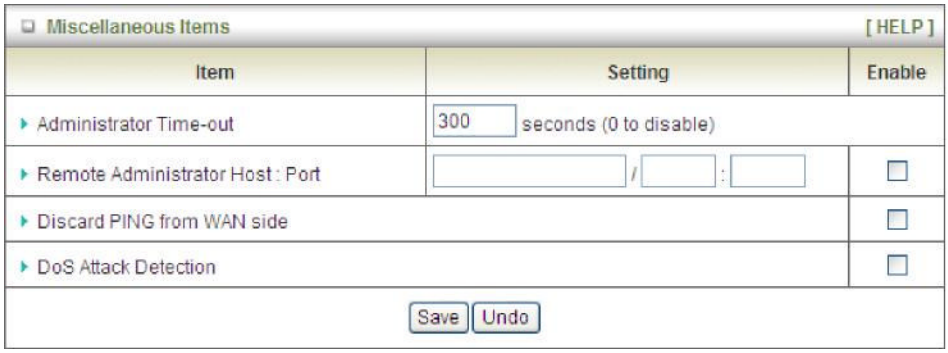
1. **MAC Address Control**: Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

2. **Connection control**: Check "Connection control" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.

3. **Association control**: Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

Click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.3.5. Miscellaneous



1. **Administrator Time-out**: The time of no activity to logout automatically, you may set it to zero to disable this feature.

2. **Remote Administrator Host/Port**

   In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".

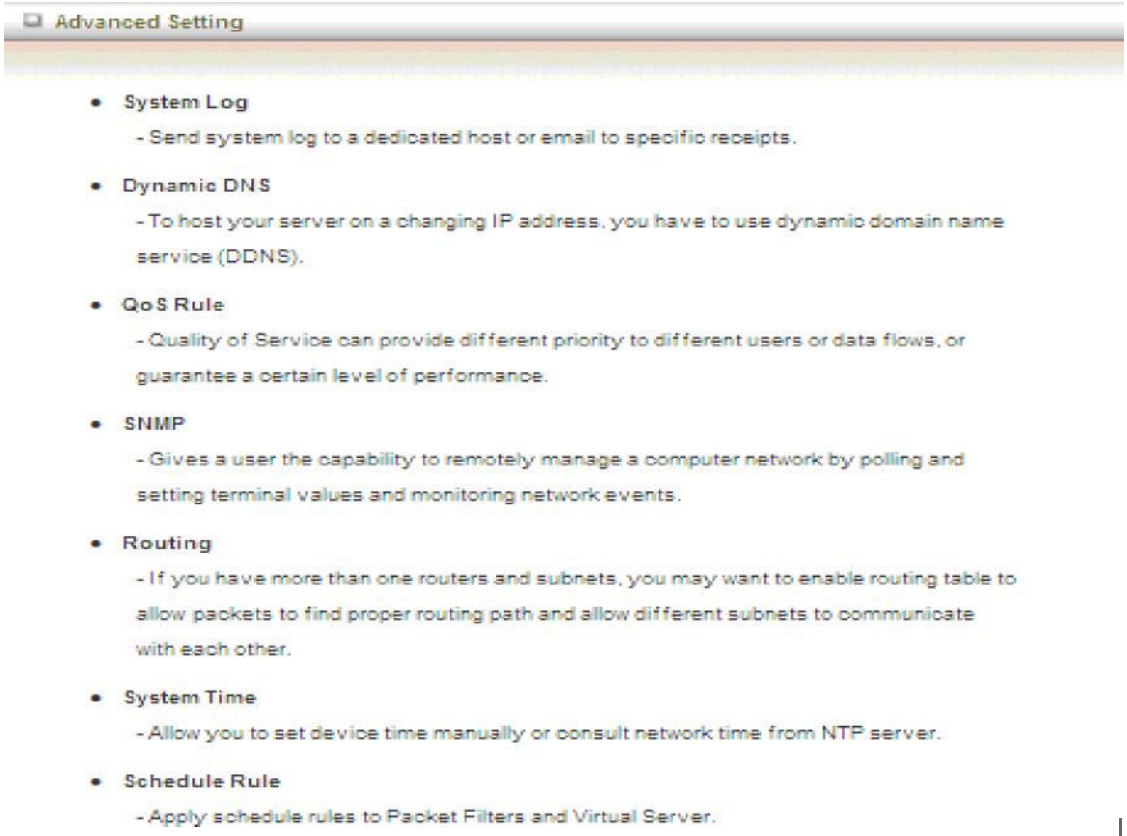
   NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

3. **Discard PING from WAN side**: When this feature is enabled, any host on the WAN cannot ping this product.

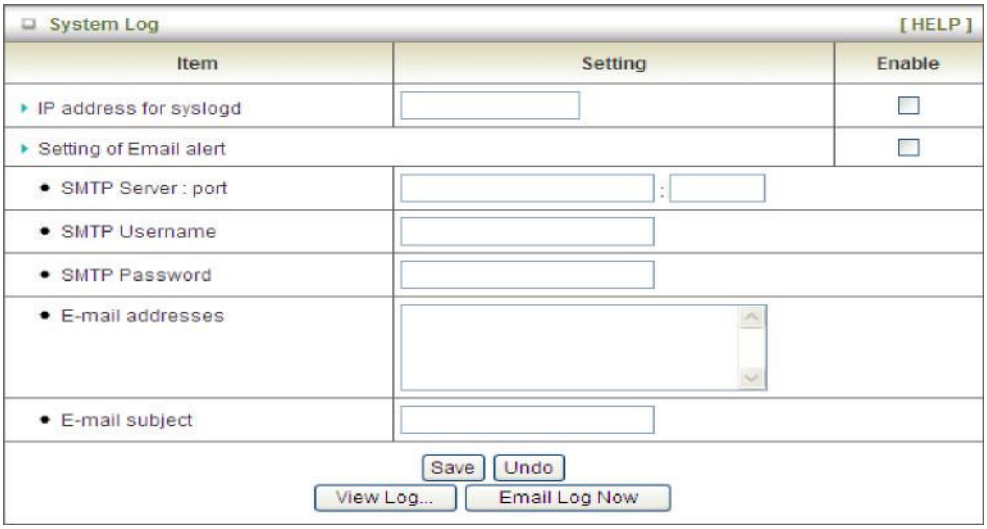
4. **DoS Attack Detection**: When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.4. Advanced Setting


Advanced Setting
System Log
- Send system log to a dedicated host or email to specific receipts.
Dynamic DNS
- To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
QoS Rule
- Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
SNMP
- Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
Routing
- If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
System Time
- Allow you to set device time manually or consult network time from NTP server.
Schedule Rule
- Apply schedule rules to Packet Filters and Virtual Server.

3.2.4.1. System Log



This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

1. **IP Address for Sys log**: Host IP of destination where sys log will be sent to. Check **Enable** to enable this function.
2. **E-mail Alert Enable**: Check if you want to enable Email alert (send syslog via email).
3. **SMTP Server IP and Port**: Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.

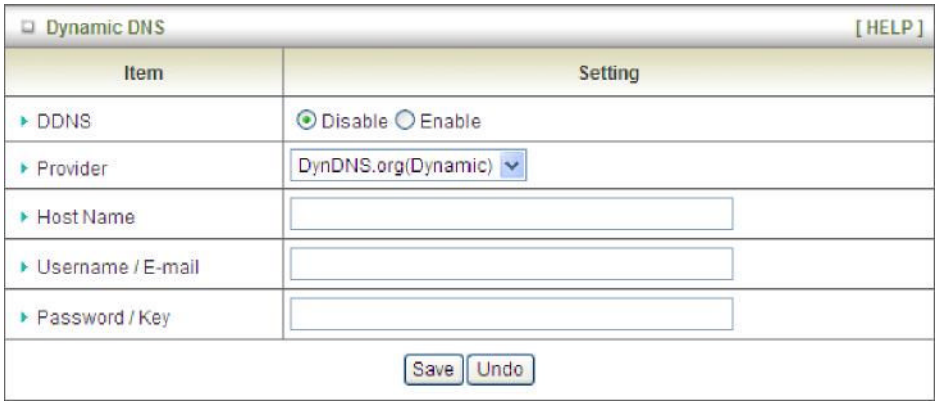
   For example, "mail.your_url.com" or "192.168.1.100:26".
4. **Send E-mail alert to:** The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
5. **E-mail Subject**: The subject of email alert, this setting is optional. **Click on**

   "Save" to store your settings or click "Undo" to give up the changes.

3.2.4.2. Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

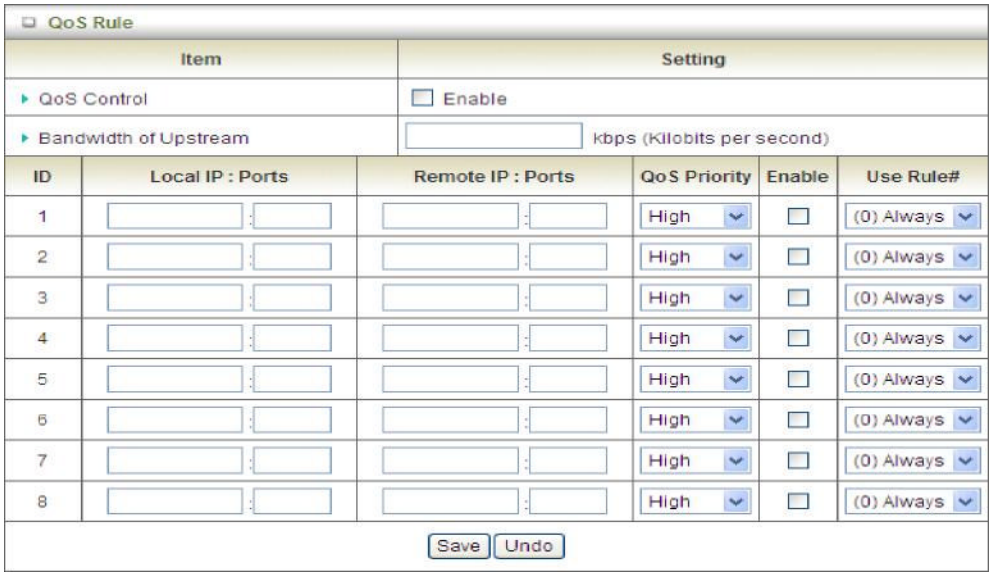
Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **Provider** field.



To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field. Next you have to enter the appropriate information about your Dynamic DNS Serve .**Provider**, **Host Name**, **Username/E-mail**, and **Password/Key**. You can get this information when you register an account on a Dynamic DNS server.

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.4.3. QOS



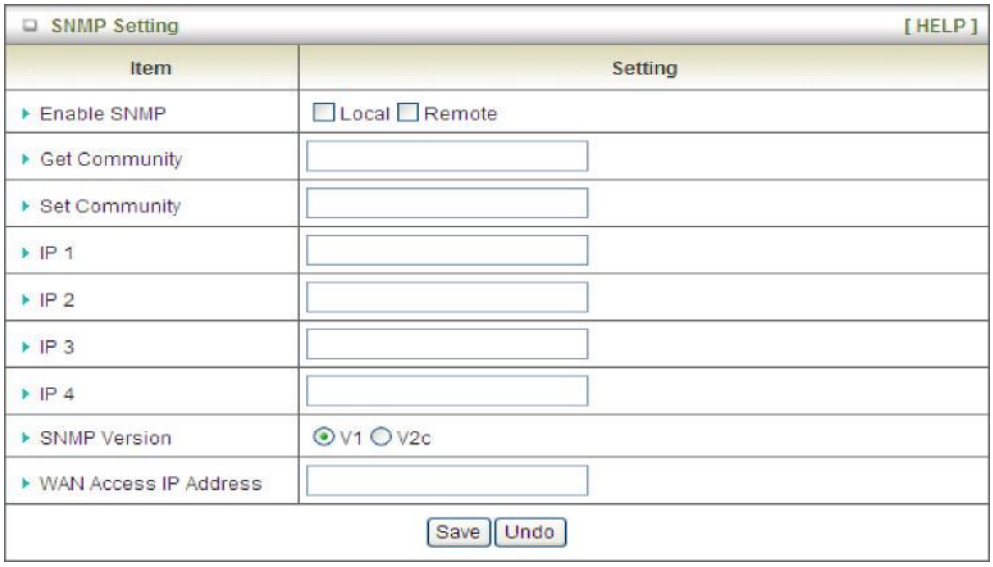
Provide different priority to different users or data flows, or guarantee a certain level of performance.

1. **QOS Control**: Check **Enable** to enable this function.
2. **Bandwidth of Upstream**: Set the limitation of upstream bandwidth
3. **Local IP : Ports**: Define the Local IP address and ports of packets
4. **Remote IP : Ports**: Define the Remote IP address and ports of packets
5. **QoS Priority:** This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal level is recommended. For non-critical applications select a Low level.
6. **Enable**: Check to enable the corresponding QOS rule.
7. **User Rule#**: The QoS rule can work with Scheduling Rule number#. Please refer to the Section 3.1.4.7 Schedule Rule.

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.4.4. SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

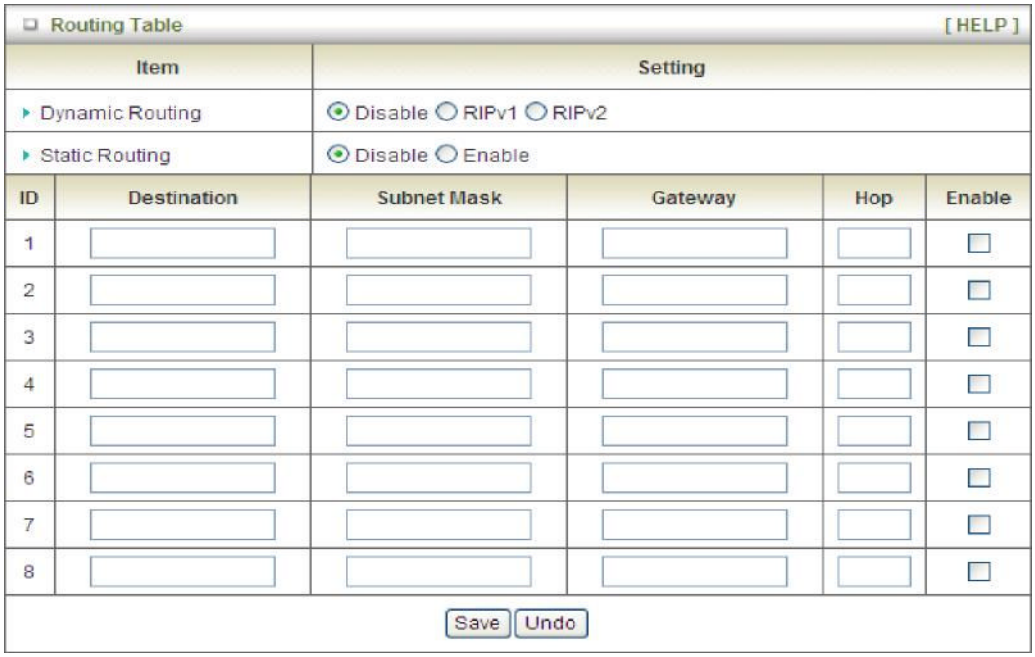


1. **Enable SNMP**: You must check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will response request from LAN. If “Remote” is checked, this device will response request from WAN.
2. **Get Community**: The community of GetRequest that this device will respond.
3. **Set Community**: The community of SetRequest that this device will accept.
4. **IP 1, IP 2, IP 3, IP 4**: Enter the IP addresses of your SNMP Management PCs. User has to configure to where this device should send SNMP Trap message.
5. **SNMP Version**: Select proper SNMP Version that your SNMP Management software supports.
6. **WAN Access IP Address**: If you want to limit the remote SNMP access to specific computer, please enter the PC’s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.

Click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.4.5. Routing

If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other. The routing table allows you to determine which physical interface address to use for outgoing IP data grams.



1. **Dynamic Routing**: Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

2. **Static Routing**: For static routing, you can specify up to 8 routing rules. You can enter the **destination IP address**, **subnet mask**, **Router**, and **hop** for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.4.6. System Time

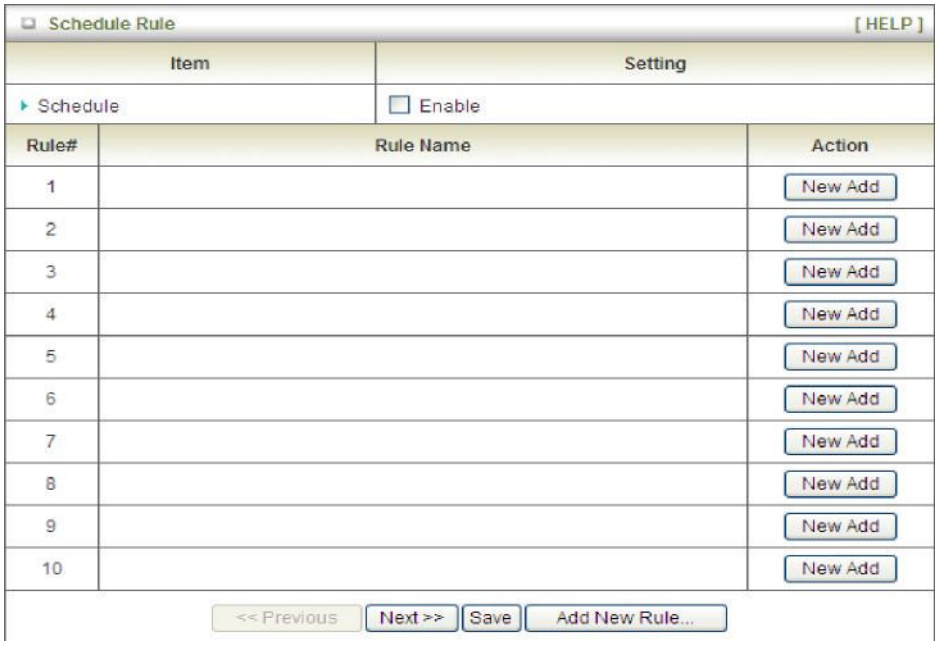
1. **Time Zone**: Select a time zone where this device locates.
2. **Auto-Synchronization**: Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server**: Click on the button if you want to set Date and Time by NTP Protocol manually.
4. **Sync with my PC**: Click on the button if you want to set Date and Time using PC’s Date and Time manually.

.

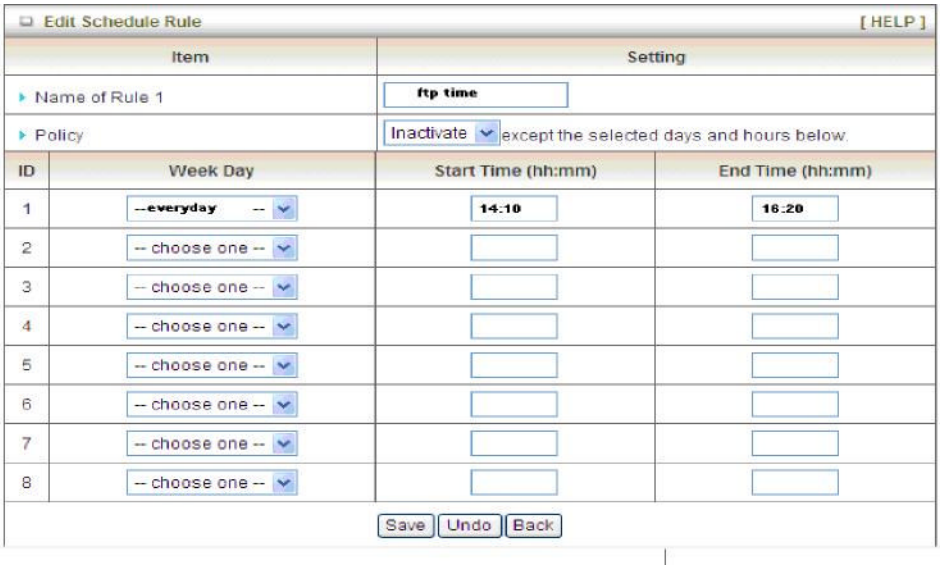
Click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.4.7. Scheduling

You can set the schedule time to decide which service will be turned on or off.

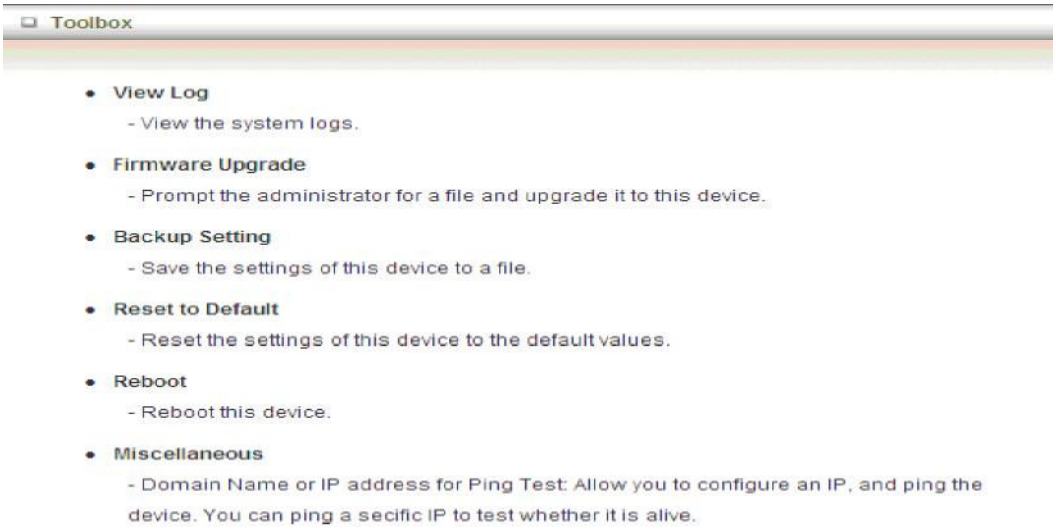


1. **Schedule**: Check to enable the schedule rule settings.
2. **Add New Rule**: To create a schedule rule, click the “Add New Rule” button. You can edit the **Name of Rule**, **Policy**, and set the schedule time (**Week day**, **Start Time**, and **End Time**). The following example configures “ftp time” as everyday 14:10 to 16:20.



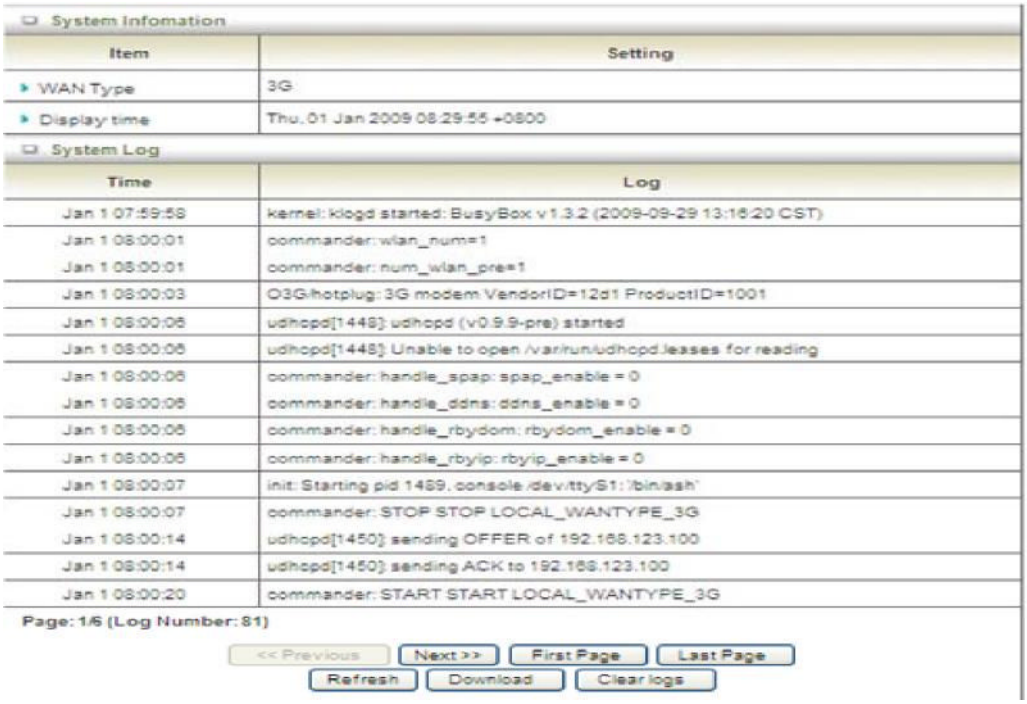
Click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.5. Tool Box

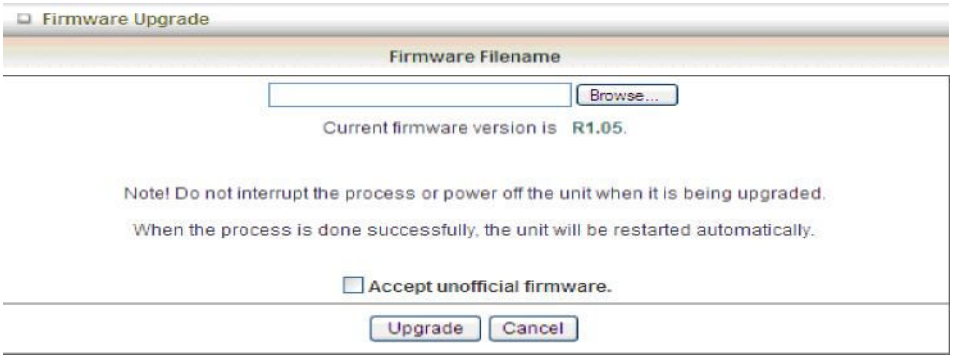

Toolbox
View Log
- View the system logs.
Firmware Upgrade
- Prompt the administrator for a file and upgrade it to this device.
Backup Setting
- Save the settings of this device to a file.
Reset to Default
- Reset the settings of this device to the default values.
Reboot
- Reboot this device.
Miscellaneous
- Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a secific IP to test whether it is alive.

3.2.5.1. System Info

You can view the System Information and System log, and download/clear the System log, in this page.

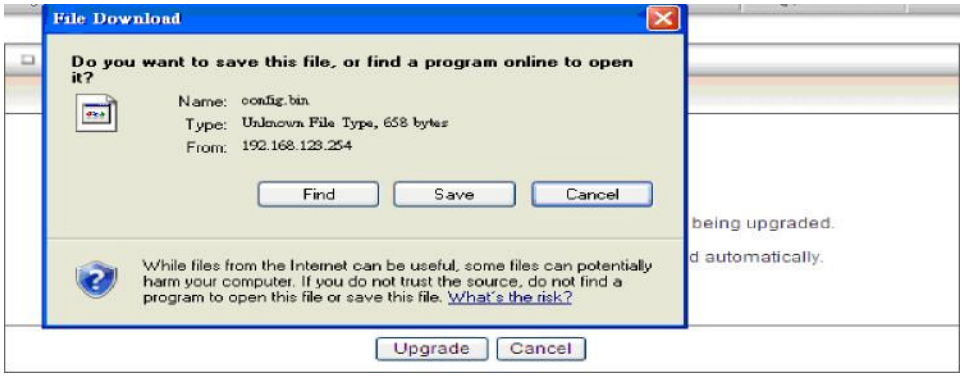


3.2.5.2. Firmware Upgrade


Firmware Upgrade
Firmware Filename
Browse...
Current firmware version is R1.05.
Note! Do not interrupt the process or power off the unit when it is being upgraded.
When the process is done successfully, the unit will be restarted automatically.
Accept unofficial firmware.
Upgrade
Cancel

You can upgrade firmware by clicking “Upgrade” button.

3.2.5.3. Backup Setting


File Download
Do you want to save this file, or find a program online to open it?
Name: config.bin
Type: Unknown File Type, 658 bytes
From: 192.168.123.254
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?
being upgraded.
automatically.
Upgrade
Cancel

You can backup your settings by clicking the “**Backup Setting”** function item and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

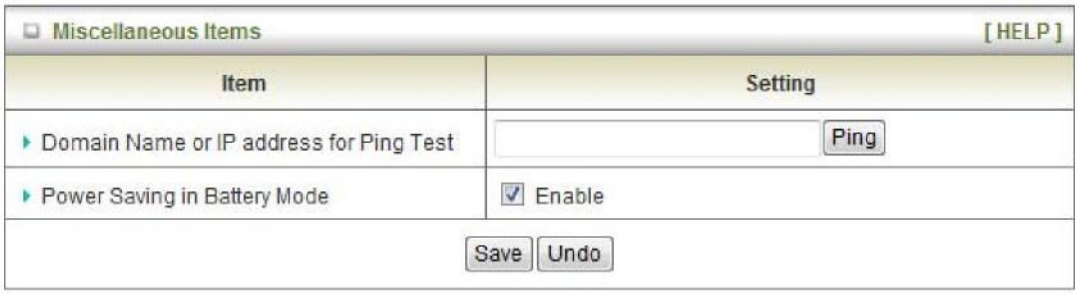
3.2.5.4. Reset to Default

You can also reset this device to factory default settings by clicking the **Reset to default** function item.

3.2.5.5. Reboot

You can also reboot this device by clicking the **Reboot** function item.

3.2.5.6. Miscellaneous



Domain Name or IP address for Ping Test

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Power Saving in Battery Mode

Enable this option to activate power saving policy when power is supplied by battery. .

4. Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the YOYORouter. You can refer to the following if you are having problems.

4.1. Basic Problems

YOYORouter does not switch on – indicator lights all off

- The battery may be fully discharged – connect the charger and try again
- The battery may be incorrectly inserted – check that the gold contacts on the battery line up with the contacts in the battery compartment

How to reset YOYORouter to factory state

Your YOYORouter can be reset to its factory state. This is useful if you have changed and forgotten the W-Fi network name (SSID) or Wi-Fi password.

To reset YOYORouter:

1. Switch on YOYORouter in Modem mode
2. Locate the Reset switch on the rear of YOYORouter B1.
3. Use a pencil or other tool, insert it in the Reset hole and gently press the Reset switch for at least 8 seconds.
4. YOYORouter restarts.

After Reset, YOYORouter will make its default configuration, which is suitable for most users. If necessary, re-configure your YOYORouter to your own needs.

The Wi-Fi network will have been changed to a network name (SSID) like **YOYORouter-12-34** where the numbers are particular to your example and printed on the label on the device itself and the carton in which it was supplied. The password is also printed on the label.

4.2. Wi-Fi Problems

I cannot find the Wi-Fi network

By default, YOYORouter's Wi-Fi network name (SSID) is like **YOYORouter-12-34** where the numbers are particular to your example and printed on the label on the device itself and the carton in which it was supplied.

- Try moving closer to YOYORouter
- On the device you are trying to connect, request it to re-scan for networks and see if YOYORouter-xx-xx appears.

If you have configured your YOYORouter to hide the SSID, it will not appear in the network list on any device you try to connect.

- You must select manual configuration and enter the network name and password.
- Or you must change the setting Advanced > Wireless > SSID Broadcast to Enable (you need a device connected to YOYORouter to be able to access the settings)

I can't connect to the Wi-Fi network

- Move YOYORouter and the wireless client into the same room, and then test the wireless connection.
- Turn off YOYORouter and the client, then restart it and then turn on the client again.
- Make sure that you have selected the YOYORouter network.
- Make sure you have entered the correct password.

- If the client device needs you to enter authentication and encryption explicitly, enter WPA2 and AES (default YOYORouter settings)
- If WPA2/AWS does not work, try WPA and TKIP (also works with default YOYORouter settings)
- Disable all security settings such as WPA and MAC Address Control. If you are now able to connect, you must re-enable security controls that work with your client.
- Ensure that the LEDs are indicating normally. If not, make sure that the AC power adaptor is connected.
- If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors…

My Wi-Fi connection drops or is unreliable

- Position YOYORouter and clients closer together
- Avoid solid walls and other obstructions which reduce the range of the Wi-Fi signal
- Try different antenna orientations for the YOYORouter – stand the device vertically for example.
- Try to keep YOYORouter at least 15cm away from the wall or other objects.
- Try changing the channel on the YOYORouter to avoid interference from other Wi-Fi networks. (By default YOYORouter tries to find a channel with low interference)
- Keep YOYORouter and clients away from electrical devices that generate RF noise, like microwave ovens, audio and TV senders, electric motors, etc.

I have lost the Wi-Fi password

- The default network password is printed on the device label and on the label affixed to the carton in which the device was packaged.

I need to connect a device that does not support WPA or WPA2 /
I want to run YOYORouter in Open or WEP security mode

YOYORouter's default configuration is to accept connection using WPA(TKIP) or WPA2(AES). To change YOYORouter to open or WEP mode:

1. Connect to YOYORouter using a device that does support WPA or WPA2 and enter the WPA password printed on the device's label, or connect using Ethernet.
2. Open the browser at 192.168.1.1,
3. Log in and use the configuration wizard or change settings Advanced > Basic > Wireless > Authentication & Encryption to suit the device that you need to connect.
4. Allow YOYORouter to reboot
5. Reconnect using the new security settings.

I changed the default Wi-Fi password and cannot remember what password I set

- You must reset YOYORouter to factory state.
- Connect using the default network password printed on the device label and on the label affixed to the carton in which the device was packaged
- Open the browser at 192.168.1.1 and log in (password: admin)
- Make any necessary configurations again using the Wizard or the Advanced configuration pages.

I cannot locate the default password for my YOYORouter

The default network password is printed on the device label and on the label affixed to the carton in which the device was packaged. If these labels are missing or damaged:

- Contact YOYOMotion. If possible please supply the MAC address, serial number or IMEI of the device in question.

I am connected to the YOYORouter Wi-Fi network but cannot access the configuration

pages
By default the configuration pages are reached by opening the browser on a connected device and selecting 192.168.1.1

- If you previously changed the IP address range, for example to 192.168.123.254, you must use this address to access the configuration pages
- If you changed the IP address and no longer know the new setting, you should perform a factory re-set and then reconfigure your YOYORouter.

4.3. Problems with the Mobile Broadband Connection

YOYORouter isn't connecting to Mobile Broadband

Basics:

- Make sure that the SIM is correctly inserted in your USB Modem
- Check on the Status page that the USB Modem is recognized by YOYORouter
- If the SIM needs a PIN code, use the configuration wizard to enter the PIN to YOYORouter.
- Check that there is mobile service at your location

The default connection profile suits most users, however you may need to select an alternative:

1. Access the configuration wizard by selecting 192.168.1.1 in your browser
2. At the 3G step, select Manual for Dial-Up Profile
3. Select your country
4. Select your mobile operator. If there are several listings, select the one that most closely corresponds with your subscription (for example, PrePay). If you have special settings or your operator is not shown, select **Others** and enter the details manually.

5. Complete the wizard
6. Allow YOYORouter to restart
7. Check if a connection can now be made.

Note: If you need to ask your mobile operator for settings, you will need the following:

- APN (Access Point Name)*
- Username
- Password
- Primary DNS
- Secondary DNS

* indicates mandatory items. In most cases only APN is needed; DNS is rarely required.

Note: the number to dial is *99#

I have set up my PIN code but YOYORouter still cannot connect

If your SIM has a PIN code, the configuration wizard may not have been able to detect the settings for the mobile operator.

- Restart YOYORouter and re-run the wizard

Or

- Configure YOYORouter manually

My Mobile Internet connection drops unexpectedly

- Position your YOYORouter so that the signal strength is as strong as possible
- Check that the **Connection Control** setting at Advanced > Basic > Network Setup > Connection Control is set to **Auto Reconnect (always-on)**

My Mobile Broadband connection is very slow (2G service)

If the connection is using a 2G network, then the very fastest you can expect is around 200kbps download (EDGE) or 54kbps (GPRS).

- Try moving YOYORouter to a window or different location to pick up a 3G signal. (3G network operate at higher frequencies which penetrate buildings less well than 2G)

By default, YOYORouter always selects a 3G network when available (auto mode). It is possible to select 2G only or 3G only service.

- Check that YOYORouter is not in Preferred Service Mode **2G Only** or **2G First;** preferred mode is **Auto Mode.**

Some network operators only provide 3G service for Mobile Broadband devices.

- You must relocate YOYORouter to a position where 3G service is available

My Mobile Broadband connection is very slow (3G service)

- Try moving YOYORouter to a window or different location to pick up stronger 3G signal.

Network Type in the Status Page indicates N/A

- YOYORouter is unable to obtain the network type (UMTS, EDGE, etc) from the USB Modem.

4.4. Other Problems

I cannot access the wizard – message "Query Status… Please wait a moment…

- You can return to the status screen by using the URL http://192.168.1.1/status.htm?rc=

My USB modem is not listed

Manufacturers sometimes produce the same device with different model numbers, for example due to case colour. Models not listed may operate due to similarity with a model that has been tested. Testing an unlisted model is at your own risk.

My USB Modem is branded by my Mobile Operator

USB modems are frequently branded by the mobile operator. Check the documentation, device labels, packaging and web support for the device, or ask your mobile operator for the generic manufacturer and model.

My USB Modem has a microSD Card slot. Can I access the card via YOYORouter EE1?

- Sorry, YOYORouter does not support this feature.

Appendix A Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux-2.6.21 system kernel

busybox - V1.3.2

BridgeUtil - bridge-utils-1.1.tar.gz

DHCP20175 - svn://busybox.net/trunk/udhcp Revision = 20175

DNRD - V2.17

IPTables142 - V1.4.2

L2TP - rp-l2tp-0.4.tar.gz

PPP - ppp-2.4.4.tar.gz

PPPoE - rp-pppoe-3.8.tar.gz

PPTP - pptp-1.7.1.tar.gz

SNMP - ucd-snmp Version: 4.1.2

IPRoute2 - http://developer.osdl.org/dev/iproute2 iproute2-2.6.11-050330

WirelessTool - wireless_tools.28.tar.gz

ZebraRouting - zebra-0.95.tar.gz

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS